普通高等学校本科专业设置申请表



校长签字：

学校名称（盖章）：武汉工程科技学院

学校主管部门：湖北省

专业名称：网络空间安全

专业代码：080911TK

所属学科门类及专业类：工学 计算机类

学位授予门类：工学

修业年限：四年

申请时间：2025-07-04

专业负责人：宋军

联系电话：15071059090

教育部制

1. 学校基本情况

学校名称	武汉工程科技学院	学校代码	13664
主管部门	湖北省	学校网址	https://www.wuhues.com
学校所在省市区	湖北武汉江夏区纸坊熊廷弼街特8号	邮政编码	430200
学校办学基本类型	□教育部直属院校 □其他部委所属院校 ☑地方院校 □公办 ☑民办 □中外合作办学机构		
已有专业学科门类	□哲学 ☑经济学 □法学 ☑教育学 ☑文学 □历史学 □理学 ☑工学 □农学 □医学 ☑管理学 ☑艺术学		
学校性质	☑综合 □理工 □农业 □林业 □医药 □师范 □语言 □财经 □政法 □体育 □艺术 □民族		
曾用名	中国地质大学江城学院		
建校时间	2004	首次举办本科教育年份	2004年
通过教育部本科教学评估类型	合格评估	通过时间	2023年04月
专任教师总数	1115	专任教师中副教授及以上职称教师数	503
现有本科专业数	44	上一年度全校本科招生人数	3320
上一年度全校本科毕业人数	2890		
学校简要历史沿革	武汉工程科技学院（原中国地质大学江城学院）创办于2004年2月，是一所经教育部批准的全日制普通本科高校。2014年5月，教育部批准学校转制并更名为武汉工程科技学院。2014年9月，学校成为湖北省首批应用型人才培养试点高校。2023年4月，学校通过教育部本科教学工作合格评估。		
学校近五年专业增设、停招、撤并情况	学校近五年增设专业12个： 机器人工程、电子商务、网络与新媒体、绘画、大数据管理与应用、人工智能、金融科技、体育教育、智能建造、物联网工程、应用心理学、艺术与科技 学校近五年停招专业14个： 国际经济与贸易、商务英语、宝石及材料工艺学、工程管理、绘画、影视摄影与制作、金融科技、工商管理、通信工程、测绘工程、地理空间信息工程、广播电视编导、摄影、电子商务		

	学校近五年撤销专业12个： 市场营销、旅游管理、地理信息科学、勘查技术与工程、地质学、资源勘查工程、测控技术与仪器、汽车服务工程、交通运输、物流管理、广播电视学、服装与服饰设计

2. 申报专业基本情况

申报类型	新增国控专业		
专业代码	080911TK	专业名称	网络空间安全
学位授予门类	工学	修业年限	四年
专业类	计算机类	专业类代码	0809
门类	工学	门类代码	08
申报专业类型	新建专业	原始专业名称	-
所在院系名称	计算机与人工智能学院		
学校现有相近专业情况			
相近专业1专业名称	计算机科学与技术（注：可授理学或工学学士学位）	开设年份	2004年
相近专业2专业名称	软件工程	开设年份	2014年
相近专业3专业名称	-	开设年份	-

3. 申报专业人才需求情况

申报专业主要就业领域	随着网络强国、数字中国、智慧社会等国家战略深入实施，网络空间安全已成为国家安全体系的重要组成部分。网络安全产业快速发展，涵盖信息基础设施保护、数据安全、工业控制安全、人工智能安全、区块链安全等多个前沿方向，对高素质网络安全专业人才的需求持续增长。 网络空间安全专业毕业生主要面向党政机关、军队公安、能源电力、通信运营商、金融机构、互联网企业、高端制造、交通运输、医疗健康、教育科研等行业单位，承担网络与信息系统安全架构设计、安全开发、攻防技术、运维管理、漏洞挖掘、安全审计、态势感知、风险评估等岗位职责。同时，毕业生还可在网络安全企业、科研机构及高校从事安全产品研发、安全技术研究和安全教育培训等工作。随着数字化转型的不断深入，网络空间安全技术将更加广泛地应用于社会治理、数字政务、智能制造、智慧城市等关键领域

	，为国家安全和数字经济发展提供有力支撑。	
人才需求情况	据中国信息通信研究院发布的《2022年中国网络安全产业白皮书》预测，到2025年我国网络安全产业规模将超过2500亿元，网络安全专业技术人才缺口将超过200万人。调研显示，各行业数字化转型速度加快，信息系统防护、数据安全、工业互联网安全、关键信息基础设施保护等领域对网络安全人才的需求持续增长，呈现出“重基础、重实践、重覆盖”的特点。 结合区域产业发展态势和学校服务地方经济的办学定位，网络空间安全专业毕业生主要面向地方通信企业、政府职能部门信息化岗位、金融与制造企业信息运维岗位、公安司法类技术支撑单位、信息安全服务公司等基层单位，从事网络与信息系统运维、信息安全管理、安全产品集成、网络攻防测试、数据安全监测、网络应急响应等相关技术与支持性岗位。 从学校历届相关专业毕业生就业情况和近年用人单位反馈看，用人单位对于基础扎实、动手能力强、具备一定实战经验和团队协作能力的网络安全初级工程师、系统维护员、安全运维员、渗透测试助理、安全合规助理等岗位需求明显增长。用人单位普遍表示欢迎具备一定攻防技能基础、熟悉主流操作系统与安全软件、掌握网络通信与访问控制原理、能执行基础安全策略配置和故障处理任务的应用型本科毕业生。网络空间安全专业具有明确的政策导向、稳定的岗位需求和广泛的行业适应性，尤其在面向区域基层单位、服务地方数字化建设方面就业前景良好。 此外，专业毕业生将以“基础型、实践型、服务型”为导向，满足用人单位对网络安全人才的多层次需求。本专业也将为学生提供继续深造的基础，部分具备较好学术能力的学生可通过考研进入信息安全、计算机技术、数字取证等相关学科方向的研究生阶段学习，拓展个人职业发展空间。	
中报专业人才需求调研情况	年度招生人数	60
	预计升学人数	6
	预计就业人数	54
	武汉佰钧成技术有限公司	7
	武汉云尚数据技术有限公司	6
	武汉光谷信息安全技术有限公司	6
	武汉优炫信息科技有限公司（武汉分部）	6
	武汉赛宁科技有限公司	5

	湖北新蓝天信息安全技术有限公司	5
	绵阳奇安信科技有限公司	5
	武汉安胜科技有限公司	4
	湖北慧拓科技有限公司	4
	武汉瀚海北斗科技有限公司	3
	武汉芯特信息技术有限公司	3

4. 产业调研报告

网络空间安全行业产业调研报告

1. 国家政策背景和产业战略

1.1 国家网络空间安全人才培养的政策背景

网络空间安全关乎国家安全和战略利益。近年来，党中央和国务院高度重视网络安全人才培养，出台了一系列政策为高校网络空间安全学科建设提供指导支持。例如，2016 年中央多个部委联合印发了《关于加强网络安全学科建设和人才培养的意见》，在全国范围推动网络安全一级学科专业和院系建设，创新人才培养机制，同时正式设立了“网络空间安全”一级学科[1]。自该学科设立以来，全国已有 60 余所高校成立了专门的网络安全学院，200 余所高校开设了网络安全相关本科专业点[1]。这体现了国家从顶层设计上完善网络安全人才培养体系的决心。此外，教育部实施“一流网络安全学院建设示范项目”，遴选重点高校率先探索网络安全卓越人才培养模式，为全国树立示范。

国家法律法规也为网络安全人才培养奠定了制度基础。《中华人民共和国网络安全法》（2017 年施行）确立了网络安全工作的法律框架，随后《数据安全法》《个人信息保护法》等法律相继出台，加强关键信息基础设施保护和数据安全管理[1]。这些法律的实施提高了全社会对网络安全的重视程度，客观上推动了对高素质网络安全人才的需求。党的二十大报告进一步强调“教育、科技、人才是全面建设社会主义现代化国家的基础性、战略性支撑”，强调网络空间的竞争归根到底是人才竞争[2]。习近平总书记多次指出要加强网络安全人才队伍建设，加快培养高层次人才，以支撑网络强国战略[2]。在这一系列指示和政策引领下，各级政府和教育主管部门加快了网络安全学科专业建设步伐，“十四五”时期网络安全人才培养进入快车道。

各地区和部门也出台配套措施推进人才培养。中央网信办等部门指导在武汉市建设国家网络安全人才与创新基地，探索“产学研”融合的人才培养新模式；工业和信息化部会同北京市打造国家网络安全产业园区，促进网络安全产业集聚发展[1]。这些举措从国家层面构建了人才培养与产业发展的融合平台，有利于形成教育培训机构与产业用人单位协同育人的良好局面。以上表明，国家政策层面

对网络空间安全本科人才培养提供了明确方向和有力支持，要求高校担当起培养网络强国建设所需人才的重任。

1.2 国家网络安全产业战略布局

网络安全产业战略与人才战略密不可分。我国自“十三五”以来将网络安全产业发展提升至国家战略高度，提出建设网络强国、数字中国的目标。在顶层设计方面，《国家网络空间安全战略》（2016 年）明确了国家在网络安全领域的发展战略和任务方向。在“十四五”规划纲要中也强调要“加强网络安全宣传教育和人才培养”，提升国家网络安全保障能力[5]。工业和信息化部、中央网信办等先后发布了促进网络安全产业发展的指导意见，如《关于加强网络安全产业创新发展的指导意见》等，部署网络安全核心技术攻关、产业生态培育等任务。这些产业政策为网络安全行业提供了政策扶持和发展机遇。

从产业布局来看，国家积极推动网络安全产业基地和集聚区建设，形成区域协调的发展格局。除前述北京的国家网安产业园、武汉的国家网安人才与创新基地外，国内还布局了成渝地区国家网络安全产业园（我国首个跨省域国家级网安产业园）等，打造区域网络安全创新高地[1]。各重点省市也结合自身产业基础出台了专项政策，支持本地网络安全企业发展和人才引进。例如，北京市网络安全产业规模已占全国 50%以上，聚集网络安全企业近千家[5]；浙江、广东等地将网络安全纳入数字经济发展规划，产业增速保持 20%以上[5]。这些举措体现出国家在产业战略上采取“重点区域引领、全国协同推进”的思路，通过政策引导和资源投入，壮大网络安全产业实力。

国家产业战略还特别关注网络安全关键领域和新兴方向的发展，以引领未来需求。例如强调加强人工智能安全、数据安全、工业互联网安全等关键技术研发，补齐产业短板[5]。近年来数据安全上升为新的国家关注重点，《数据安全法》实施后，各行业对数据安全解决方案和合规服务需求激增，网络安全产业新增的增长点集中在数据安全、云安全、个人隐私保护等领域[2]。这直接带动了相关人才需求的扩大。国家层面的产业战略方向为高校的人才培养指明了重点领域，高校应据此调整专业设置和课程内容，注重培养在数据安全、人工智能安全等新兴方向具备专长的人才。

总体而言，国家网络空间安全人才培养政策和产业发展战略相辅相成：政策为人才培养提供了制度保障和目标要求，产业战略为人才施展才干提供了广阔舞台和明确方向。高校在这样的背景下，应顺应政策导向、贴合产业需求，培养出德才兼备、能满足国家战略和产业发展需要的网络安全专业人才。

2. 全国、湖北省及武汉市网络安全产业发展趋势

2.1 国家网络安全产业发展概况

近年来，中国网络安全产业蓬勃发展，市场规模持续扩大。根据中国网络安全产业联盟数据，2022 年我国网络安全市场规模达到 633 亿元人民币，同比增长 3.1%，并预计未来三年将保持高速增长。随着数字化转型的深入推进，市场需求将持续旺盛，预计 2023 年市场规模将增至 728 亿元，2024 年有望达到 837 亿元，2025 年更将突破 963 亿元，年均增速保持在 15%左右，展现出巨大的增长潜力和广阔的发展空间。这些预测数据综合了行业报告和市场分析，详见中国网络安全产业联盟 2024 年报告[5]以及 IDC、Gartner 等权威机构的市场预测[8].

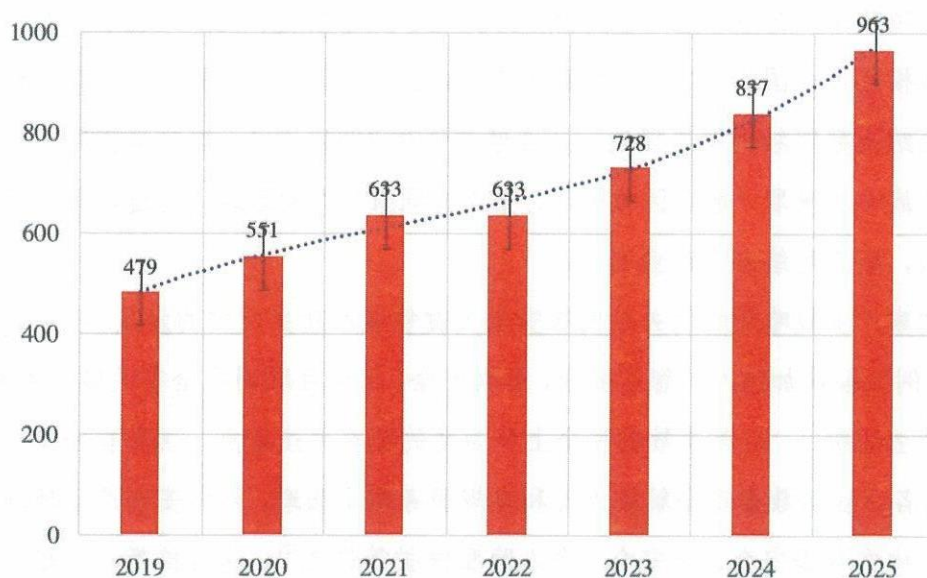


图 1：2019 – 2025 年中国网络安全市场规模及预测（人民币亿元）。其中，2019 – 2024 年数据根据公开报告整理 ；2025 年为预测值。可以看出我国网络安

全产业规模在经历早期高速增长后，近期增速有所放缓，但总体仍保持上升趋势，并预计在“十四五”末突破 900 亿元大关。

产业发展驱动力方面，数字经济和新技术应用成为网络安全产业的新引擎。云计算、大数据、5G、人工智能等新兴技术的广泛应用，一方面提升了企业运营效率，另一方面也带来了新的安全威胁，迫使企业加大安全投入[5]。尤其是数据要素的价值提升使数据安全成为热点领域，《数据安全法》《个人信息保护法》的实施推动各行业建立数据安全和隐私保护机制，直接催生了对数据安全产品与服务的巨大需求。网络安全产业正从传统的边界防护，延伸到数据安全、云安全、物联网安全、工控安全等多个新赛道，行业呈现多元化发展的新态势[5]。例如，人工智能安全近年来成为研究焦点，AI 技术应用同时伴生安全挑战，催生了对 AI 模型安全、防对抗攻击等方面的需求[5]。可以预见，随着数字化、智能化深入，各类新技术新应用都将不断提出新的安全需求，推动网络安全产业持续演进。

从行业结构看，目前我国网络安全产业仍以传统安全产品为主，但服务化趋势在增强。网络安全用户主要集中在政府、通信、金融等行业，三者合计占市场收入的 58.4%[5]。头部企业具有明显优势，据统计奇安信、启明星辰、深信服、天融信等四家龙头企业的市场占有率均超过 5%，多数头部企业收入增速高于行业平均水平[9]。同时，大批中小安全企业在近五年涌现：截至 2022 年底，全国经营数据安全相关业务的企业数量已超过 25 万家，且 2018－2022 这五年成立的企业占 90%[5]。这说明网络安全产业创业创新活跃，新进入者众多，但也反映出许多企业规模较小、竞争力有待提升的问题。未来产业或将经历从“遍地开花”向“做大做强”的转变，预期头部厂商将通过技术和资源优势巩固市场地位，中小企业则需走专精特新道路寻求差异化生存。

2.2 湖北省网络安全产业发展现状

湖北省作为中部地区科教和产业大省，近年来在网络安全产业方面也取得了显著发展。根据赛迪顾问的区域竞争力研究评估，湖北近年来加速布局网络安全领域，产业发展较快，已跻身全国网络安全产业竞争力的第二梯队[5]。尤其是依托省会武汉的综合优势，湖北正逐步形成网络安全产业集聚。在工业和信息化部等部委的支持下，武汉市东西湖区建设了国家网络安全人才与创新基地，经过七

年发展，该基地已成为全国唯一集“网络安全学院+创新产业谷”于一体的基地，支撑起国家“网络强国”战略在中部地区的实施[9]。

目前武汉临空港经开区的国家网安基地已初具规模：全国网络安全50强企业有一半落户于此，集聚了上下游相关企业超过200家，建设有12家研发中心[9]。基地内网络安全产业形成了网络应用安全、通信安全、数据安全、自主可控等四大领域方向，串联起“基础软硬件—安全设备—安全软件—安全服务—安全应用”的完整产业链[9]。这一集群被形象地称为“中国网谷”，其聚集效应正不断增强。多家知名网络安全企业（如中金数据、天融信、数字认证等）相继在武汉布局运营，带动了本地产业规模和技术水平的提升[9]。根据地方媒体报道，武汉市网络安全及相关产业年产值近年来突破了200亿元规模，产业生态日趋完善。湖北省经信厅也将网络安全产业列为全省战略性新兴产业链进行重点培育，出台措施支持本土网络安全企业发展壮大[9]。

在人才和创新方面，湖北省依托科教资源优势推进产学研协同。武汉国家网安基地不仅聚集企业，还引入了武汉大学、华中科技大学的网络安全学院入驻办学，培养高层次创新型人才[9]。基地成立以来已举办各类网络安全意识提升和技能培训活动200余期，培训人数超过2.5万人次[5]。此外，湖北围绕顶尖网络安全人才、领军人才的引进出台了专项支持政策，力图将武汉打造成国家网络安全人才高地[5]。截至2023年，湖北省拥有的网络安全从业人员数量在1万余人规模，在全国处于中上水平[5]。全省有15所高校开设了网络安全相关专业，为产业输送人才。这些数据表明湖北在网络安全人力资源储备方面具备一定基础。

总体来看，湖北省网络安全产业呈现出“政府引导、企业集聚、校企合作”的良好态势。本省既有国家级产业基地这样的载体平台，又有武汉大学等高校智力支持，再加上区位辐射中西部的市场潜力，未来有望在全国网络安全版图中占据更重要的位置。湖北需要继续发挥自身科教和产业优势，加强政策扶持与招商引资，推动本地网络安全企业技术创新，打造在中部领先的网络安全产业集群。

2.3 武汉市网络安全产业基础与集群

武汉市作为湖北省会和中部特大城市，是全省乃至中西部地区网络安全产业发展的核心引擎。武汉的网络安全产业基础雄厚：一方面，武汉科教资源丰富，

有武汉大学、华中科技大学等重点高校设有网络安全学院或相关学科，为本地培养和吸引了大量专业人才；另一方面，武汉的产业体系完备，信息通信、电子制造、金融等行业发达，这些行业对网络安全有大量需求，带动了安全企业在汉集聚。

国家网络安全人才与创新基地是武汉发展网络安全产业的旗舰项目。该基地坐落于武汉临空港经开区，在国家层面部署下建设。基地以“人才”和“创新”为核心功能，一方面与知名高校合作培养高端网络安全人才，另一方面引入企业研发中心和孵化项目，形成教育和产业无缝对接的格局[9]。例如，自2020年武汉大学和华中科技大学的网络安全学院搬入基地以来，已联合企业开展科研项目340余项、校企合作项目100余项[9]。基地还建设了大规模网络靶场和培训中心，联合360、奇安信等20家培训机构开展专业培训和攻防演练，提高在校生和从业人员的实战能力[9]。这一系列举措使武汉在网络安全人才培养和技术创新方面走在全国前列。

武汉市政府近年也持续发力，将网络安全产业纳入城市产业规划予以重点扶持。武汉实施了战略性新兴产业倍增计划，将网络安全与信息化作为重点方向，提出到2025年建成全国网络安全产业高地的目标[5][9]。“中国网谷”作为城市新名片，多次在政府工作报告和招商推介中被提及，显示了武汉高位推动网络安全产业的决心。市级层面成立了网络安全产业推进专班，定期举办武汉网络安全创新论坛等活动，营造产业发展氛围[9]。通过政策引导和市场机遇，武汉正吸引越来越多网络安全企业和项目落地。例如，国内知名安全厂商奇安信集团于2021年在武汉设立华中地区总部；安恒信息公司也在汉成立子公司拓展业务。据不完全统计，截至2023年，武汉市聚集的网络安全及相关企业数百家，涵盖产品研发、安全服务、密码技术、人才培训等多个领域，产业生态日趋丰富。

综合来看，武汉市在网络安全产业方面已建立起人才培养、技术创新和企业集聚三位一体的发展体系。依托国家级基地和本地综合优势，武汉有条件承载国家网络安全战略任务，成为中部地区的“网络安全枢纽”。未来随着各项建设的推进和更多企业的入驻，武汉的网络安全产业集群有望进一步壮大，在全国占据更加重要的位置。这种产业集群效应也将为本地高校网络空间安全专业学生提供更多实习实践和就业机会，形成良性循环。

3. 网络空间安全岗位需求与就业趋势分析

3.1 人才需求数量与增长趋势

当前我国网络空间安全人才市场呈现出需求旺盛但供给不足的状态。央视网在 2023 年国家网络安全宣传周期间报道的数据显示，目前我国每年网络安全人才的需求数量接近 5 万人，而高校相关专业毕业生年供应量只有约 3 万人，每年存在约 2 万人的人才缺口[3]。也就是说，仅以年度增量来看，教育系统培养的人才远不能满足当年新增的岗位需求。这一供需缺口还在进一步拉大。有研究预计，到 2025 年我国网络安全人才缺口将达到百万级别，接近 2027 年预测值 327 万人的水平[3]。另一项调查则指出，截至 2021 年我国网络安全人才总缺口约为 150 万人，预计到 2027 年这一数字将扩大到 300 万[4]。可见从总量上看，我国网络安全从业人员储备相比实际需要存在巨大不足，人才培养亟需提速。

人才需求的增长一方面源自网络安全产业自身快速发展，另一方面也与网络安全威胁形势日趋严峻有关。当下各行各业都在加强数字化和网络化建设，这使网络安全岗位渗透到更多领域。据统计，截至 2023 年，全国网络安全从业人员总数已超过 200 万人[2]。用人需求除了来自传统的 IT 和通信企业，也大量来自金融、能源、制造、政府机关等需要保护自身数字资产的单位。地域分布上，网络安全人才需求主要集中在一线和新一线城市。据调研数据，北京、上海、深圳、广州、成都、杭州六大城市提供了全国约 75%的网络安全岗位需求[2]。北上广深由于聚集了大量互联网和金融总部，对安全人才的需求长期旺盛，成都和杭州作为新兴网络安全产业高地，需求也快速攀升。这种地域集中趋势说明大型发达城市对专业人才具有更强吸引力，也反映出其他地区在网络安全人才招募上面临更大挑战。

从用人单位类型看，不同行业的网络安全岗位需求规模有所差异。政府部门和公共事业单位一直是网络安全人才的重要雇主，占据了约 24%的市场岗位需求；紧随其后的是金融行业，占比约 17%[2]。运营商和互联网企业的需求也非常可观。而随着数据安全、工控安全等新领域受到重视，工业企业和新兴技术公司对于网络安全专业人才的需求正在迅速增长。总体而言，“十四五”时期我国网络安全人才需求将保持高速增长态势，无论是数量上还是种类上都会进一步扩大和丰富。

这既给人才培养带来压力，也提供了前所未有的机遇——网络空间安全专业的毕业生将拥有广阔的就业空间和多样的职业选择。

3.2 岗位类别与技能要求

网络空间安全领域的岗位类型多种多样，不同岗位对从业者的技能要求有所侧重。根据《网络安全产业人才发展报告（2023年版）》对企业招聘需求的分析，目前企业最主要需求的岗位包括：网络安全工程师、安全运维工程师、网络安全研究员、应用安全工程师、网络安全顾问、渗透测试工程师、数据安全工程师等[2]。这些岗位几乎涵盖了网络安全工作的各个方面，既有偏向防守和运维的角色，也有偏向攻击测试的角色，还有聚焦新兴领域数据安全的角色。各岗位职责侧重不同，相应要求的知识技能也不同：

（1）网络安全工程师：定位为通用性较强的岗位，通常负责组织内部整体的安全防护体系建设和日常安全事务。此岗位要求掌握宽泛的安全知识面，包括风险评估、漏洞扫描、安全加固、应急响应、等级保护合规等多方面技能[2]。很多中小企业不会严格区分网络安全工程师和安全运维工程师，两者工作内容有交叉。因此企业更看重从业者全面的基础知识和技能广度，而对年资要求相对较低，通常1-3年经验即可胜任[2]。

（2）安全运维工程师：主要负责网络与系统的安全运行维护，保障基础设施和业务系统的安全稳定。其技能要求和网络安全工程师类似，也是需要较全面的安全知识，但更强调对系统、网络设备的配置加固和安全监控能力。由于不少企业将安全运维与安全工程师角色合并，因此具备网络管理和系统管理背景的人员转岗安全运维较为常见。

（3）应用安全工程师：专注于应用系统和软件开发环节的安全保障。该岗位对专业技能深度要求较高，需要具备安全开发方面的专长。典型技能包括制定和完善安全编码规范、为开发团队开展安全培训、进行威胁建模、安全设计评审，以及推动SDL（安全开发生命周期）在开发流程中落地等[2]。应用安全工程师必须对常见漏洞原理和防御方法有深入理解，具有实际编程和代码审计能力，以便从源头上保障应用安全[2]。

（4）渗透测试工程师：扮演“模拟黑客”的角色，对系统进行攻击性测试以发现安全漏洞。此岗位要求精通各种攻击技术和工具，具备攻防对抗的实战能力。渗透测试工程师需要掌握漏洞利用原理、风险评估方法，并能在测试后指导修复漏洞、优化安全措施[2]。由于渗透测试技术更新快、专业门槛高，企业通常要求从业者有较深入的安全研究功底和实践经验，包括参加过攻防演练或 CTF 竞赛等经历。

（5）网络安全研究员：从事安全产品技术研发、漏洞挖掘、安全策略研究等工作。此岗位通常存在于安全厂商或大型企业的安全研究团队，对从业者的理论基础和创新能力要求高。网络安全研究员需要深入理解网络安全技术发展趋势，掌握逆向分析、漏洞挖掘、密码学等高阶技能，并具备较强的科研能力以提出新思路、新工具。通常要求硕士及以上学历或同等经验。

（6）网络安全咨询顾问：为用户单位提供安全咨询、风险评估和解决方案策划的角色。顾问需要对产业和技术发展有宏观把握，以资深视角识别客户需求并设计解决方案[2]。这要求其不仅精通安全技术，还熟悉合规标准和管理体系，沟通和文案能力也很重要。网络安全顾问往往由具有多年实战经验的人员担任。

（7）数据安全工程师：这是近年来新出现的岗位，随着数据成为关键生产要素而诞生。数据安全工程师主要负责企业的数据分类分级、安全治理、隐私合规等工作，要求兼具合规意识与攻防技术。该岗位需要熟悉《数据安全法》等法规标准，懂得数据生命周期的安全风险管控，同时具备一定的渗透测试和安全开发能力，以落实对数据的全方位保护[2]。可以说数据安全工程师是“技术+管理”复合型人才，在当前企业迫切开展数据安全与隐私合规的背景下，这类岗位的人才尤为短缺[2]。

以上各岗位所需的核心技能不尽相同，但也有一些共性要求。首先，扎实的计算机基础（包括网络原理、操作系统、编程等）是所有安全岗位的必备基础[2]。统计显示，大约 32%的网络安全从业者来自计算机科学与技术、信息安全、网络工程等相关专业背景[2]。其次，实践动手能力极为重要。调查发现，从业人员工作中所用的技能有近四成来自工作项目中的经验积累，约三成通过业余自学获得，而仅有 12.64%来源于在校学习[2]。这表明网络安全岗位对实践经验的依赖度很高，用人单位往往更青睐具备实战技能的人才。再次，持续学习更新能力也是必要的

软技能。安全技术日新月异，从业者需要不断通过自学或培训跟进行业动态，以避免知识老化[2]。总体而言，网络空间安全岗位对人才的知识结构要求“广度+深度”兼备：既要有宽广的计算机和安全基础知识面，又在特定岗位方向有深入钻研的专业技能，这是高校人才培养需要努力的方向。

3.3 就业市场趋势与人才流动

网络空间安全人才的就业市场近年持续升温，就业形势十分火热。一方面，就业岗位数量快速增长，如前文所述每年新增需求数以万计，并且出现很多新兴职位；另一方面，就业质量也相对较高，表现在薪资待遇优厚（后节详述）和人才流动趋于理性等方面。

根据猎聘网发布的报告，网络安全从业者的平均跳槽周期为 4.09 年，明显高于全行业平均的 3.57 年[4]。这意味着网络安全人才整体稳定性较好，从业者更愿意在一个岗位持续发展，不会过于频繁地更换工作。这与网络安全岗位具有较强专业性的特点有关：一名安全工程师熟悉一家企业的系统后，其价值会随经验积累而提高，同时行业内资深人才紧缺，用人单位也会通过加薪留人。因此网络安全领域的人才流动相对稳定，不像某些 IT 岗位存在频繁跳槽现象。这对于用人单位来说是有利的，能够培养和留住骨干力量，但同时也使得外部招聘高级安全人才变得困难，企业更倾向于从头培养新人或内部提拔。

人才地域流动方面，如前述，大城市集聚效应明显。很多网络安全专业毕业生倾向于前往北京、上海、深圳等一线城市就业，以获取更高薪酬和更好的职业发展机会[2]。相对而言，中西部地区和中小城市由于产业机会相对较少，招揽高端安全人才比较困难，不少岗位存在“招不到合适人”的情况。这也促使一些用人单位尝试通过远程招聘或外包方式解决安全人才不足的问题。但对于涉及核心安全岗位的工作，大多还是要求驻场并确保可信任度。因此，人才向发达地区流动的趋势短期内难以逆转。对于我们地方高校而言，一个对策是加强与省内外优势企业合作，搭建实习实践渠道，让学生在校期间与大厂建立联系、提升能力，这样毕业时无论选择留在本地还是去外地，都更具就业竞争力。

值得注意的是，网络安全人才的职业发展路径也在逐步拓宽。传统上，技术路线人才做到一定资历，可以成长为安全架构师、安全专家等高端岗位；而管理

路线则可以成为安全部门负责人（如CISO首席信息安全官）等。随着网络安全地位提升，许多大型机构设立了CISO或等同职务，高级安全管理人才有了清晰的晋升空间。另外，网络安全创业也方兴未艾，不少有经验的技术人才选择创办自己的安全公司或咨询业务。政府事业单位也增加了网络安全职位的编制投入。种种迹象表明，网络空间安全领域不仅“就业易”，而且“发展好”，能够为人才提供长远的职业成长空间。这也是吸引更多优秀学生报考和投身该领域的一个重要因素。

3.4 薪资待遇水平分析

网络空间安全人才的薪资待遇在IT行业中名列前茅，具有明显的竞争优势。根据BOSS直聘发布的网络安全人才趋势报告，2021年网络安全领域平均招聘月薪达到18627元，是全行业平均水平的2.4倍[4]。其中，核心技术研发类安全人才的平均月薪更高，约为21182元[4]。相较而言，全国各行业岗位平均招聘月薪大约在7500元左右[4]。由此可见，网络安全专业人才的收入水准远高于多数其他行业。图2直观比较了网络安全与全行业平均薪资的差异。

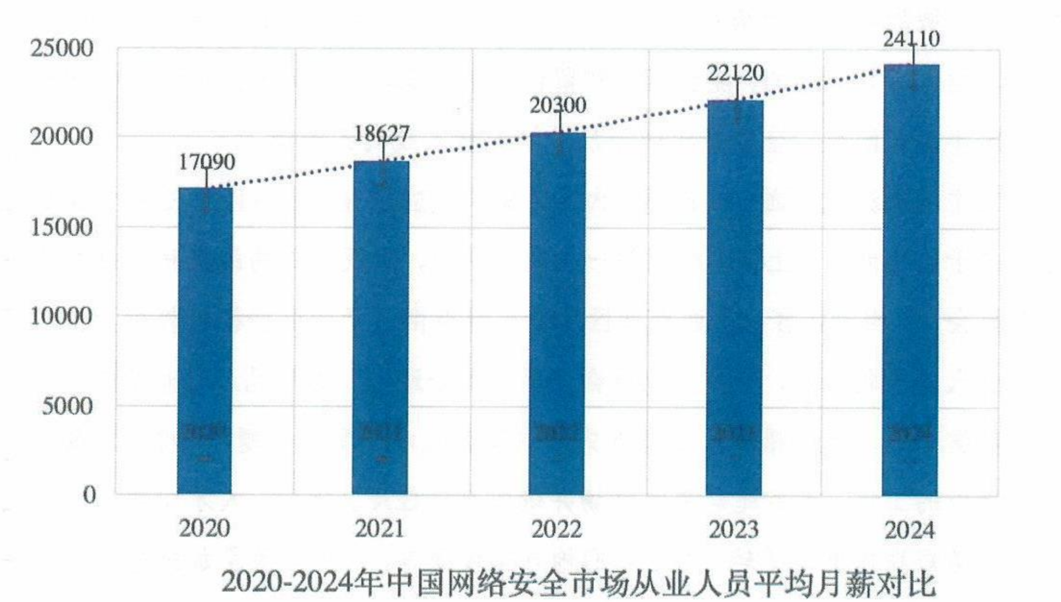


图2：平均月薪对比（2021年数据）。网络安全领域平均招聘月薪约18627元，全行业平均约7755元，核心安全研发岗位平均可达21182元。网络安全人才薪酬显著高出社会平均水平，体现出其供需紧张和高技能价值。

除了平均薪资高，网络安全岗位的薪资上升通道也较为通畅。初级安全工程师岗位的起薪普遍在 8K－12K 元/月左右，而具备 3－5 年经验的中级工程师薪资可达 15K－20K+。在一线互联网大厂或金融机构，资深安全工程师的月薪甚至可以超过 30K。有报道指出国内安全岗位的最高月薪记录达到 47.3K[10]，显示顶尖人才炙手可热。在管理层面，安全主管或经理级别年薪通常在几十万元区间；而“首席信息安全官（CISO）”等高管岗位年薪则可达数十万美元级别[10]。例如国外大型企业中 CISO 年薪范围在 10 万-50 万美元[10]。虽然国内尚未完全与国际接轨，但一线互联网公司的安全负责人年薪百万人民币以上已较为常见。

薪资待遇的节节攀升，正是由于网络安全人才供不应求导致的人才竞争加剧。企业为吸引和留住安全人才，不惜开出优厚条件，包括高薪资、股票期权、培训机会等。尤其在具备实战能力的紧缺型人才（如高级渗透测试工程师、数据安全专家）方面，薪酬水准水涨船高。一些核心技术岗位甚至出现了“逆向挖人”的现象：安全厂商愿意出更高薪去从甲方企业挖安全负责人，反映出对优秀人才的渴求。根据智联招聘的数据，近年来安全岗位的求职者期望薪资也在上升，2021 年求职者期望平均月薪已达 14013 元，而用人单位给出的平均月薪为 11555～13398 元左右，供需双方在薪酬上仍存在一定差距[4]。但总体看，这一领域的高薪趋势短期内不会改变。

对于高校毕业生而言，网络空间安全专业可谓就业“高薪黄金岗”。高薪资不仅是对个人价值的肯定，也吸引更多优秀青年进入这一领域，从而形成正循环。当然，需要注意的是，高薪伴随高要求，雇主对人才技能和经验非常看重。因此毕业生要想拿到理想的薪酬，在校期间就应努力提高实战能力和项目经验，以匹配企业的需求标准。

4. 湖北省高校相关专业设置情况分析

4.1 本科层次网络空间安全及相关专业分布

湖北省在网络空间安全及相近专业的高等教育布局上已有相当基础。根据教育部高校专业设置数据统计，湖北省开设“信息安全”本科专业的院校有 12 所，在全国各省中位居前列[2]。此外，湖北省开设“网络空间安全”本科专业的院校

目前有5所左右，包括武汉大学、华中科技大学、武汉工程大学、湖北工程学院、武汉东湖学院等[6]。下面列出湖北省部分高校及其开办的网络安全相关本科专业：

表1：湖北省部分高校网络空间安全及相关专业设置概览。

学校名称	本科专业设置
武汉大学	信息安全、网络空间安全（设有国家网络安全学院）
华中科技大学	信息安全、网络空间安全（设有网络空间安全学院）
武汉工程大学	网络空间安全
湖北工程学院	网络空间安全
武汉东湖学院（民办）	网络空间安全
中国地质大学（武汉）	信息安全
湖北大学	信息安全（设有网络空间安全学院）
湖北工业大学	信息安全
湖北警官学院	网络安全与执法（公安类专业）

从上表1可以看出，湖北省的网络空间安全本科教育既有传统“双一流”高校的参与（如武大、华科），也逐步扩展到地方普通高校和民办高校。武汉大学和华中科技大学是湖北最早开设网络安全相关专业的高校，分别于2001年和2016年设立了信息安全和网络空间安全专业，并且两校都获批参与国家一流网络安全学院建设项目，在全国具有示范作用。近年来，一些应用型本科院校也开始增设该专业，如武汉工程大学和湖北工程学院分别于2020年前后获教育部批准增设网络空间安全本科专业[6]。民办本科武汉东湖学院也抢抓机遇开办了网络空间安全专业，以满足社会对人才的迫切需求[6]。另外，在公安政法领域，湖北警官学院开设的“网络安全与执法”本科专业则侧重培养网络犯罪侦查和执法人才，这是安全学科与法学交叉的一个独特方向，目前全省仅此一所[7]。由此可见，湖北高校在本科层面已形成了一定规模的网络安全人才培养体系，覆盖了研究型、应用型和行业特需等不同层次。

除了本科教育，湖北的高职高专院校在网络安全相关专业上也有所布局。据统计，湖北省有20余所高职院校开设了“信息安全与管理”或“信息安全技术

应用”等专科专业[7]。例如，武汉软件工程职业学院、襄阳职业技术学院、湖北职业技术学院等都设有信息安全类专业。这些高职院校每年也为本省输送一批面向基层一线的信息安全技术人才，缓解了基础岗位的人才紧缺。总体而言，湖北省从专科到本科各层次已经较为完备地布局了网络空间安全及相关专业点，为本地网络安全产业发展提供了人才支撑。

然而，相对于快速增长的人才需求，湖北高校的人才培养规模仍显不足。据央视报道，全国高校每年输出约 3 万名网络安全相关毕业生[3]。按湖北在全国的办学占比推算，湖北地区每年毕业的网络安全专业本科生大约在千人规模上下。这与全省每年上万的人才需求相比（如前述湖北从业人员 1 万余人[5]，且大部分在武汉市集中需求），仍存在相当差距。因此湖北高校有进一步扩容相关专业招生、增加培养数量的必要。同时，在专业分布上也存在不平衡现象：绝大多数优质网络安全本科教育资源集中在武汉市，省内其他地市如襄阳、宜昌等地缺乏本科层次的网络安全专业点。这可能导致人才地域分布失衡，大部分毕业生留在武汉或外流，而地市州机关企事业的网络安全岗位招不到人。这些问题都需要通过优化专业布局和加强区域合作来逐步解决。

4.2 同类院校专业设置对比

为了评估武汉工程科技学院开设网络空间安全本科专业的必要性，我们有必要对比分析省内同类型院校在该领域的专业设置情况。武汉工程科技学院作为一所应用型本科高校（民办），其“同类院校”主要是指湖北省内定位相近的地方普通本科院校和独立学院/民办本科院校。例如湖北工程学院、武汉东湖学院、湖北文理学院、武汉纺织大学等在办学层次和服务面向上与我校相近。

从上述列举看，湖北工程学院和武汉东湖学院均已设立了网络空间安全本科专业，走在了应用型院校的前列。湖北工程学院是省属本科院校，在孝感市，2021年开始招生网络空间安全专业，体现了地市高校对培养本地网络安全人才的重视。武汉东湖学院作为民办高校，也较早响应市场需求开办了该专业。除此之外，湖北文理学院（襄阳）目前尚未开设独立的网络空间安全专业，但其计算机学院下设有信息安全相关方向课程。武汉纺织大学等工科院校也暂未见正式设置该专业的信息。不过，这些院校都有计算机科学、网络工程等专业基础，未来增设网络

安全专业具有潜力。可以预见，随着网络安全重要性的提高，省内会有更多应用型本科高校尝试申请增设该专业，区域竞争将逐渐显现。

相比之下，我校（武汉工程科技学院）目前尚未开设网络空间安全或信息安全方向的本科专业，这在省内同类院校中已略显滞后。从学校发展战略考虑，为了保持竞争力、满足社会需求，我校有必要尽快启动网络空间安全本科专业的建设申请。通过调研我们也发现，一些已经设立该专业的兄弟院校在办学过程中积累了可供借鉴的经验。例如，他们大多依托学校原有的计算机类学科基础，组建由计算机专业教师+外聘安全专家组成的师资队伍；在课程设置上注重实践环节，与企业合作建立实训基地或工作室；在招生宣传上突出“高就业、高薪资”的专业吸引力，录取分数逐年提高。这些做法对于我校将来办专业具有参考价值。

在专业定位上，不同层次高校也有所差异。像武汉大学这类“双一流”高校的网络空间安全专业偏重学术研究和国家高端人才培养，而应用型院校则更注重培养面向企业一线的实践型人才。我校如果设立该专业，应当明确走应用技术型路线，突出实践教学和技能训练，使毕业生胜任各类企事业单位的安全管理和技术支持岗位。这与我们学校的办学定位是吻合的。我校多年来在工科实践教学方面有一定优势，如果将这种优势延伸到网络安全领域，完全可以形成自身的特色与竞争力。

总的来说，湖北省内已有部分同类院校抢先开设了网络空间安全本科专业，取得了良好反响。我校若不及时跟进，可能在新兴专业竞争中处于不利地位。引进并建设该专业，将有助于完善我校的学科专业布局，提升学校在信息技术领域的影响力，同时也满足区域对网络安全人才的需求。因此，对标同类院校，我校开办网络空间安全专业既有压力也有动力，我们应认真分析他们的经验教训，找准自身切入点，办出特色来。

5. 本校设立网络空间安全本科专业的必要性与可行性

5.1 必要性分析

结合以上调研，可以总结出我校申请增设网络空间安全本科专业的几大必要性：

（1）服务国家战略和地方需求的需要。 网络空间安全是国家重大战略需求领域，人才培养被提升到前所未有的高度[2]。作为高校，有责任响应国家号召，为网络强国建设贡献力量。我校增设该专业，能够培养本地区的网络安全人才储备，服务国家安全战略。同时，立足湖北和武汉来看，网络安全产业在本地快速发展，企业对人才求贤若渴，每年数以千计的岗位空缺[3]。当前湖北省网络安全人才供给不足，每年约 2 万人的缺口需要更多高校来分担培养任务[3]。我校位于武汉，直接面向本地产业，可以就近为武汉的国家网安基地及众多企事业单位输送人才。因此，开设网络空间安全专业对接区域经济社会发展需求，具备迫切性和现实意义。

（2）完善学科专业布局、提升办学层次的需要。 我校目前已有计算机科学与技术、软件工程等相近专业，这些专业与网络空间安全关系密切。开设网络空间安全本科专业有助于完善我校的信息技术学科版图，形成“计算机+网络安全”相互支撑的发展格局。通过新专业建设，可以促进相关学科的交叉融合，催生新的教学和科研增长点。同时，网络安全属新兴热门专业，社会关注度高，办好这个专业有望提高我校的知名度和美誉度，带动招生就业的良性循环。对于我校这样一所应用型本科院校来说，增设符合时代需求的新专业是提升办学层次、打造办学特色的重要举措，可有效提高学校在同类院校中的核心竞争力。

（3）顺应学生兴趣和就业“风口”的需要。 当前信息安全、网络安全已成为青年学生普遍关心的领域，“网络安全人才缺口大、待遇好”的信息也广为流传。不少理工科学生对网络攻防、黑客技术等充满兴趣。如果我校有网络空间安全专业，能够吸引这部分有志于网络安全事业的优质生源，满足他们的求知欲和成才愿望。从就业看，网络安全岗位薪资高、职业发展好，是名副其实的“就业风口”专业[4]。开办该专业，将为我校学生拓展一条高质量就业的新通道，提高毕业生就业竞争力和就业满意度。这对学生、家长和学校都是有利的，因此从人才培养的角度也是很有必要的。

（4）弥补本校专业设置空白、发挥自身优势的需要. 我校在工科教育方面有一定办学基础，尤其在计算机、电子信息类专业上积累了师资和实验室条件。但目前还没有专门面向网络安全方向的本科专业，这是我们专业布局上的一个空白点。填补这一空白，可以将我校现有的计算机网络、通信技术、信息管理等学

科资源加以统筹利用，产出新的成果。一方面，我们有多名计算机相关专业的骨干教师，经过进修培训后可以转型从事网络安全课程教学，教师队伍比较容易搭建；另一方面，我校原有的计算机网络实验室、信息系统实验室等，经过适当升级改造即可支撑网络安全实践教学，不需要完全从零开始建设。因此，我们具备将现有资源升级应用于新专业的优势条件。只要论证通过并科学规划，我校完全有能力依托既有基础成功开办网络空间安全专业，这也是发挥学校潜力、实现自身发展的需要。

（5）缓解区域人才紧缺、履行社会服务职能的需要。 武汉作为中部网络安全人才高地，目前高校中虽然有武大华科等培养一批高端人才，但大量中小企业和基层单位更需要应用型的网络安全工程技术人才。这部分人才的供给主要依赖地方高校。正如前文分析，湖北省许多地市尚缺乏网络安全本科教育资源，毕业生多流向省会，大量本地岗位难招人。我校若开设该专业，可在一定程度上缓解区域特别是武汉市及周边对应用型网络安全人才的紧缺状况，为本地留住人才。作为一所扎根湖北的高校，培养服务地方的网络安全专门人才是我们义不容辞的社会责任。这不仅响应了政府关于高校服务地方发展的号召，也将提高学校对区域经济社会的贡献度和影响力。

以上种种因素表明，我校申办网络空间安全本科专业具有现实而紧迫的必要性。这既是顺应国家和时代发展的要求，也是学校自身内涵建设和外延发展的需要，可谓水到渠成、势在必行。

5.2 可行性分析

在确认了必要性的同时，我们也需要理性评估我校开办网络空间安全本科专业的可行性，即办好这个专业所具备的基础条件和可能面临的挑战。总体来看，通过前期调研和自我诊断，我们认为我校具备开设该专业的基本条件，项目可行，但仍需在若干方面加以加强和保障：

师资力量： 我校现有计算机类相关专业专任教师 82 人，其中具有副高及以上职称的 32 人，博士学位教师 7 人。这支队伍中，不乏研究方向涉及信息安全、网络技术的教师。一部分教师已具备教授网络安全基础课程的能力。此外，我们在武汉的人才环境中，可以通过柔性引进和兼职聘任的方式，吸纳行业企业的一

线安全专家和工程师担任实践课程导师。例如，与武汉本地网络安全企业合作，邀请其资深工程师担任校外指导教师。目前武汉的国家网安基地聚集了众多安全厂商，为我们聘请兼职师资提供了便利条件[9]。只要学校在人事政策上给予支持，“专兼结合”的师资队伍是可以迅速组建起来的。当然，我们也需制定师资培训计划，选派现有青年教师赴知名高校进修网络安全方向课程或参加教育部组织的师资培训班，以尽快提升专任教师的专业水平。这些工作已经在调研阶段引起重视，学院层面表示有信心在1-2年内打造出一支合格的网络安全教学团队。

课程与教材： 网络空间安全专业的核心课程体系包括密码学、计算机网络安全、操作系统安全、网络攻防技术、应用系统安全、数据库安全、恶意代码分析等。这些课程我校过去虽未系统开设过，但我们可以借鉴兄弟院校的成熟方案来构建课程体系。教育部高等学校网络空间安全专业教学指导委员会已发布了网络空间安全专业的教学标准和指南，各高校也公开了人才培养方案。这为我们设计课程提供了依据。在教材方面，国内已有一批权威教材可供采用，例如《网络安全概论》《密码学与网络安全》《Web安全攻防实战》等等。同时，我们计划与合作企业共同开发校本案例教材，将实践项目融入教学[2]。 指出应“推进校企合作，鼓励企业与院校共同制定培养方案、开发教材”，我们完全可以按此思路实施[2]。因此，课程和教材准备上不存在无法克服的困难，可行性高。

实验实训条件： 开办网络安全专业需要建设相应的实验室和实训平台。我校目前拥有的计算机实验中心可以作为基础，增加部分网络安全设备和软件平台后加以利用。具体来说，我们拟新建/改建如下实验条件：（1）网络攻防实验室：配备隔离的内部实验网络、攻击测试主机、防火墙、安全扫描器等设备，用于渗透测试和攻防演练教学；（2）数据安全与密码实验室：配备密码算法实验套件、数据库安全实验平台等；（3）安全运维综合实训平台：模拟企业IT环境，部署态势感知系统、SOC安全运营平台，供学生实训。初步预算这些实验室建设需要资金320万元，学校财务显示可以通过专项经费和企业共建方式筹措。我们已与武汉某网络安全企业初步洽谈对方援建实验室事宜，对方有意向捐赠一批安全设备用于教学。鉴于我校与企业合作历来紧密，实训条件保障总体可行。

生源和就业： 从招生角度看，网络空间安全专业属于理工类中的热门方向，预计每年在湖北省的本科招生中都能吸引足够考生报考。我校近几年在同批次院

校中生源情况稳定，如果增设该专业，将成为新的增长点。通过宣传其良好就业前景和高薪资吸引力，相信能获得考生和家长的积极响应。在就业方面，我们有地处武汉的区位优势，可以直接对接国家网安基地和各用人单位。前期调研中，武汉多家信息安全企业表示非常欢迎本地高校培养的应用型安全人才，希望能建立毕业生输送合作关系。一些企业愿意提供带薪实习岗位，提前与学生签约。鉴于每年省内毕业生有限，行业对口单位众多，我们有理由相信本专业毕业生就业会呈现供不应求的态势，就业质量有保障。这种良好预期也进一步论证了开办的可行性。

管理与持续发展：学校层面对新专业建设高度重视，已经成立了由校领导牵头的专业建设论证工作组，统筹调配资源。学院也制定了详细的建设规划，包括师资培训、课程开发、实验室建设、校企合作等时间表。有了学校的支持和明确的规划，新专业从申报到落地执行有可靠的组织保障。当然，我们也认识到专业建设是长期过程，需要持续投入和改进。例如在师资梯队培养上，要建立青年教师培养机制，使得专业能可持续地发展壮大；在科研上，要鼓励专业教师申报网络安全方向的课题，提升学术水平，从而反哺教学。这些都需要学校在政策和经费上给予倾斜。从目前沟通情况看，校方对此是有充分认识并愿意投入的。

总之，经过客观评估，我们认为武汉工程科技学院具备开设网络空间安全本科专业的可行性：有相关学科基础可依托，有师资和实验条件可以整合提升，有明确的培养定位和方案，有市场需求和就业渠道做支撑。在充分准备的前提下，申报该专业是可操作且有望成功的。当然，我们也将秉持“务实低调”的态度，不夸大不冒进，一步一个脚印地把专业建设好，确保真正培养出高质量的人才，向社会和主管部门交出满意的答卷

6. 人才培养方向规划与行业发展潜力展望

6.1 人才培养模式和方向规划

在明确开办网络空间安全专业的必要性和可行性之后，关键是要做好实际的人才培养工作。为此，我们根据调研结果和行业需求，提出如下人才培养模式和方向的规划：

(1) 坚持实践导向，强化实战能力培养。 调研反映，目前高校网络安全毕业生普遍存在实践动手能力不足的问题，42%的院校尚未开展网络攻防实验或开展不足[3]。对此，我们建议在人才培养方案中大幅提高实践教学比重。例如，每门核心专业课都配套相应实验或项目任务，增设独立的网络攻防实训课程。同时，建设校内网络靶场环境，定期举办校园攻防演练和CTF比赛，以赛促学，培养学生的实战技能。另外，安排至少半年的企业实习，选派学生到网安基地内的企业实训，直接参与实际安全项目。这些举措将使学生毕业时具备较强的实战本领，能够无缝对接企业需求[3]。企业专家指出，要尽快建立网络安全人才实战能力评价体系[3]，高校可与行业协会合作，对学生实战能力进行测评认证，倒逼教学改革。

(2) 创新校企合作的人才培养模式。 网络空间安全是实践性很强的学科，必须走产教融合道路才能提高培养质量[2]。我们建议与本地网络安全龙头企业共建产业学院或实践基地，实行“双主体”育人。一方面，邀请企业深度参与人才培养方案制定、课程开发和教学实施。例如，与企业合作开设“安全运维实务”“渗透测试案例分析”等实训课，由企业工程师授课[3]。另一方面，实施订单式培养，针对特定企业岗位需求联合培养学生，毕业直接上岗。还可以探索“学徒制”模式，学生在校学习与企业见习交替进行。在教材和资源方面，与企业联合开发具有企业真实案例的教材和题库。通过以上措施，充分发挥企业在培养过程中的作用，确保学生所学即企业所需，实现学以致用。

(3) 突出新兴方向，打造专业特色。 如前文行业趋势分析，数据安全、云安全、物联网安全、工控安全等是当前热点和人才缺口所在[2]。因此我校在专业方向上积极响应这种趋势，形成特色。具体做法包括：在课程设置上新增数据安全与合规、云计算安全、工业控制系统安全等选修模块，培养学生在新兴领域的意识和技能；鼓励师生围绕这些方向开展项目研究和大创课题，形成特色成果；邀请相关领域的专家来校开设讲座或短课，让学生接触前沿动态。通过有意识地强化新兴方向教育，我校毕业生将在某些细分领域具备特长。例如，培养一批熟悉《数据安全法》要求、懂技术也懂合规的数据安全专才，以满足企业亟需[2]。又如，依托武汉本地的光电子和制造业基础，培养懂工控安全的人才服务工业企

业。这样的专业特色既对接产业发展需要，也有助于我校在激烈竞争中形成差异化优势。

(4) 注重交叉培养，提升综合素质。 网络安全工作往往需要复合型知识结构，如既懂 IT 又懂法律，既懂技术又善管理等。为此，我们建议在人才培养中融入交叉学科内容。一方面，加强与法学、管理学等学院的协作，开设网络法律法规、安全管理体系等通识课程，培养学生的法律意识和管理思维，使其未来能胜任安全管理、顾问等岗位[2]。另一方面，引导学生选修数学、人工智能等课程夯实理工基础，尤其是密码学需要较强的数学功底。此外，要培养学生的沟通写作能力和团队协作精神，这对安全顾问、安全管理等岗位非常重要[2]。可以通过布置文档报告撰写任务、模拟应急响应演练等方式，提高学生的软技能。总之，专业教育不能仅局限于技术本身，还应拓宽视野，培育学生成为能够沟通业务和技术的综合性人才。

(5) 完善激励机制，吸引和鼓励优秀学生深造。网络空间安全作为国家急需领域，高层次人才同样紧缺[2]。我们在本科阶段除了培养应用型人才，也应鼓励部分学有余力的学生继续攻读硕士、博士，成长为安全科研或战略人才。为此，学校可设立网络安全专业奖学金，对学业成绩或竞赛表现优异者给予奖励，激发他们深造的动力。同时，与武汉大学等开设有硕士点的高校建立推免或联合培养合作，为本科毕业生升学创造条件。这样既提高学生个人发展，长远也有利于提升学校办学层次和学术水平。

综上所述，在人才培养上我们将采取“实践为本、校企融合、新兴导向、交叉融合、激励提升”的策略，全面提高培养质量。通过这些努力，力争将本专业办出特色、办出成效，培养出符合国家和行业要求的高素质网络安全人才，为学校赢得口碑。

6.2 行业发展潜力展望

着眼未来，网络空间安全行业的发展潜力巨大，前景十分光明。这进一步坚定了我们开设该专业、培养相关人才的信心。根据行业白皮书的分析，我国网络安全市场正稳健增长，2023 年市场规模约 640 亿元，预计到 2028 年将超过 1000 亿元[10]。可以预见，未来数字经济越发展，网络安全投入就会越成为刚需，行业

规模有望持续攀升。同时，随着技术进步，新的安全领域和业态会不断出现，为人才提供新的用武之地。例如，人工智能的广泛应用将催生AI模型安全、防对抗样本攻击等新课题；元宇宙、区块链的发展也需要相应的安全防护；汽车智能网联、智慧城市等领域的安全需求将蓬勃兴起。所有这些都昭示着网络空间安全行业将长期保持朝阳态势，成为IT领域最具活力和挑战的方向之一。

从人才角度看，网络安全人才竞争将进一步加剧。据世界经济论坛的报告，亚太地区网络安全人才短缺最为明显，其中中国缺口尤为庞大[5]。企业为争夺优秀人才会持续提高待遇和福利，给予更大发展空间。这意味着本专业毕业生在未来很长一段时间内都将处于就业卖方市场，拥有良好的职业选择。另一方面，也会倒逼高校不断扩大培养规模和提升质量，以缓解供需矛盾。我们预计，国内开设网络空间安全相关专业的高校数量还将持续上升，到“十四五”末可能翻倍增长。在此过程中，办学质量高、特色鲜明的院校将脱颖而出，成为行业人才培养的重要基地。我校若能抓住机遇，在专业建设中精耕细作，有望跻身全省乃至全国网络安全人才培养的生力军，为行业输送更多栋梁之才。

网络空间安全行业未来的发展还将更加注重国际合作与对话。网络威胁无国界，国际社会对于网络安全人才的争夺和合作都会加强。一些国内优秀人才可能走向国际舞台参与全球网络安全治理，而国外先进经验也会引入国内。我们的学生应该具备一定的国际视野和交流能力，这需要我们在教学中适当加入国际标准、国外案例等内容。未来不排除有出国深造或海外就业的机会，我们也应鼓励学生去开拓。

最后，随着全社会网络安全意识的提升（全民国家安全教育的推进[1]），网络安全将像食品安全、环境安全一样成为公众日常关切的话题。这种社会环境对于网络安全行业是利好，将吸引更多人才投身其中，也促进行业地位提高和资金投入增加。网络空间安全不再是小众领域，而将成为数字时代的基础性行业之一。可以说，其发展潜力几乎与整个数字经济的发展同频共振，前途不可限量。

综上所述，我们对于网络空间安全本科专业的人才培养和行业前景保持乐观预期。在国家政策指引和产业蓬勃发展的双重推动下，我们完全有理由相信，通过科学论证和精心筹备，武汉工程科技学院网络空间安全本科专业的设立将取得成功，所培养的人才必将在国家网络安全事业和数字经济建设中发挥重要作用。

我们将本着务实进取的态度，把这一专业打造成我校新的品牌和增长点，为国家、为湖北输送源源不断的网络安全青年英才！

参考文献：

1. 中央网信办：《共筑网络安全屏障——我国网络安全工作取得积极进展》，新华网，2023年9月。

2. 工业和信息化部人才交流中心：《网络安全产业人才发展报告（2023年版）》，电子工业出版社，2023年9月。

3. 央视网：《网络安全人才每年缺口达2万人 专家建议尽快制定实战能力评价体系》，2023年9月13日。

4. 界面新闻：《领跑各大行业，网络安全人才平均年薪37.33万元，人才缺口达150万》，2021年9月15日。

5. 安全内参：《赛迪顾问：中国网络安全区域竞争力研究》，2024年5月20日。

6. 教育部学信网专业库：《开设网络空间安全专业的大学名单》（更新至2024年5月）。

7. 掌上高考：《湖北哪些专科（高职）有信息安全技术应用专业》（2025年更新）。

8. Gartner：《全球信息安全和风险管理技术服务支出预测，2023-2027》，市场研究报告 #G00789012，2023年6月。

9. 湖北日报. 武汉：撑起“网络强国”的中部脊梁[N/OL]. 人民网湖北频道，2023-05-20[2025-07-07]. http://hb.people.com.cn/n2/2023/0520/c192237-40423634.html.

10. Python84310366. 网络安全工程师前景怎么样？2024年网络安全行业分析[EB/OL]. CSDN博客，2024-06-25[2025-07-07]. https://blog.csdn.net/Python84310366/article/details/144747755.

5. 申请增设专业人才培养方案

网络空间安全专业本科人才培养方案

一、专业名称与代码

专业名称：网络空间安全（Cyberspace Security）

专业代码：080911TK

二、培养目标

网络空间安全专业立足国家网络强国战略，面向数字经济与信息社会发展需求，培养德智体美劳全面发展，具备良好政治素养、人文修养和身心素质，具有家国情怀、国际视野、工程意识和可持续发展理念的高素质工程应用型人才。毕业生应系统掌握数学与自然科学基础知识、网络空间安全领域的基本理论、核心技术与工程方法，能够在信息安全、数据安全、系统安全、应用安全等方向从事系统开发、运维管理、攻防对抗与安全服务等工作。

毕业生在完成本科学业后5年左右，预期能达到以下目标：

培养目标1 知识目标：掌握网络空间安全、计算机科学与技术、通信工程、密码学及信息系统相关基础知识与专业知识，理解网络空间安全理论体系与法律法规，具备从事复杂网络空间安全问题分析与解决的专业基础。

培养目标2 能力目标：具备良好的工程实践能力与技术整合能力，能够应用信息安全技术、软硬件开发工具及工程管理方法，进行复杂系统的安全架构设计、安全运维、攻防对抗与综合测试；能在企事业单位、政府机构及科研单位从事网络安全相关工作。

培养目标3 素质目标：具有高度的政治素质和职业道德，具备服务国家战略与行业发展的责任感和使命感，能够有效沟通、协同工作，具备终身学习的意识和能力。毕业生应在专业岗位上发挥骨干作用，部分学生应具备升学深造、技术引领或基层管理的潜质，成为具备工程素养与创新精神的新时代网络空间安全人才。

三、毕业要求

网络空间安全专业毕业生应在思想政治、人文素养、专业知识、工程

能力、沟通协作与终身发展等方面全面发展，达到以下六个方面的毕业要求：

毕业要求1 思政素养与社会责任

指标点1-1 思政认知：具有坚定的理想信念、良好的思想品质和正确的价值观，具备服务国家网络安全战略的使命感，践行社会主义核心价值观。

指标点1-2 职业伦理与规范：具有良好的职业道德，了解网络安全从业者应遵守的行为规范和职业责任，能够在实际工作中履行网络空间治理中的法律与伦理责任。

指标点1-3 社会影响与可持续发展：了解网络安全对社会、经济、环境与国家治理的深远影响，关注技术发展带来的伦理与安全问题，能够在实际工作中体现社会责任与可持续发展意识。

毕业要求2 专业基础与工程分析

指标点2-1 基础与专业知识：掌握数学、自然科学与网络空间安全相关的基础理论与专业技术，理解加密算法、访问控制、系统安全等关键知识体系。

指标点2-2 问题识别与分析：具备发现、识别和分析网络空间安全问题的能力，能够应用安全建模、漏洞分析、渗透测试等技术手段提出合理解决方案。

指标点2-3 法规与标准理解：理解网络安全相关的国家政策、行业标准、法律法规，能够在遵循规范的前提下开展系统设计与技术实现。

毕业要求3 工程能力与技术实现

指标点3-1 系统开发与运维：具备构建、部署和维护安全系统的能力，掌握常用开发工具、安全测试平台与主流安全框架。

指标点3-2 研究与分析方法：能够基于科学方法设计安全实验、分析数据、整合信息，从而得出有效的工程结论。

指标点3-3 工具与平台应用：熟练使用安全评估工具、态势感知系统及安全运维平台，理解其技术原理与适用范围。

毕业要求4 项目管理与组织协调

指标点4-1 项目原理理解：了解网络安全工程的生命周期管理过程，掌握项目评估、风险控制与成本分析方法。

指标点4-2 多学科项目应用：具备在多学科背景下开展安全项目规划与组织的能力，能够协调资源、优化流程，推动项目有效实施。

毕业要求5 沟通表达与团队合作

指标点5-1 技术交流：能够准确表达网络安全工程问题与解决方案，具备撰写技术文档、报告及进行清晰演讲的能力。

指标点5-2 团队协作：具备良好的合作精神，能够胜任项目团队中的不同角色，具备国际视野与跨文化沟通能力。

毕业要求6 学习能力与职业发展

指标点6-1 学习意识：认识到网络空间安全技术更新迅速，具备自我驱动的学习意识和信息获取能力。

指标点6-2 学习能力与适应能力：能够通过自主学习或进修不断更新知识体系，适应行业发展趋势和岗位变化，具备成长为网络安全骨干或行业技术专家的潜力。

四、主干学科

计算机科学与技术、信息与通信工程、网络空间安全

五、核心课程

计算机组成原理、数据库原理及应用、操作系统原理、网络空间安全导论、密码学基础、计算机网络安全、操作系统安全、网络攻防与渗透技术、软件安全与逆向分析、通信原理、web安全技术

六、主要实践性教学环节

AI大模型应用（训练营）、C语言课程设计、网络空间安全工程与应用、专业综合实训（产教融合）、生产实习（产教融合）、毕业实习、毕业设计（论文）

七、学制及授予学位

学　　制：四年

授予学位：工学学士学位

八、课程结构学时学分及毕业学分要求

总学分：170	必修学分、比例（%）	选修学分、比例（%）	理论学分、比例（%）	实践学分、比例（%）	学时（周数）	
					理论	实践
通识教育平台	50/29.4%	3/1.8%	40/23.5%	13/7.6%	696	268
专业教育平台	63/37.1%	20/11.8%	64/37.6%	19/11.2%	1024	304
实践教学平台	30/17.6%	0	0	30/17.6%	0	40W
个性化发展平台	0	4/2.4%	0	4/2.4%	0	4W
合计	143/84.1%	27/15.9%	104/61.5%	66/38.5%	1720	572+44W
总计	170/100%		170/100%		2292+44W	

毕业学分要求：在毕业时应达到德育培育目标和大学生体质健康标准，应获得总学分170学分，其中通识教育53学分，专业教育83学分，实践教学30学分，个性化教育4学分。

九、培养计划进程表

课程类型		课程属性	课程名称	学分	学时	学时分类		学期及学分								考核方式	开课单位
						讲课	实践	一	二	三	四	五	六	七	八		
通识教育平台	思政课模块	必修	思想道德与法治	3	48	40	8	3								考试	马院
		必修	中国近现代史纲要	3	48	40	8		3							考试	马院
		必修	马克思主义基本原理	3	48	40	8			3						考试	马院
		必修	毛泽东思想和中国特色社会主义理论体系概论	3	48	40	8				3					考试	马院
		必修	习近平新时代中国特色社会主义思想概论	3	48	40	8				3					考试	马院
		选修	“四史”课程	1	16	16	0		1							考查	马院
		必修	形势与政策	2	64	64	0	0.5	0.5	0.5	0.5					考查	马院
		小计		**18**	**320**	**280**	**40**	**3.5**	**4.5**	**3.5**	**6.5**	**0**	**0**	**0**	**0**		
	语言课模块	必修	大学英语 I	3	48	32	16	3								考试	人文学院
		必修	大学英语 II	3	48	32	16		3							考试	人文学院
		必修	大学英语III	3	48	32	16			3						考试	人文学院
		必修	大学英语IV	3	48	32	16				3					考试	人文学院
		小计		**12**	**192**	**128**	**64**	**3**	**3**	**3**	**3**	**0**	**0**	**0**	**0**		
	身心	必修	军事理论	2	36	36	0	2								考查	马院/学工

	健康模块	**必修**	大学生心理健康	2	32	16	16		2							考查	马院/学工
		必修	国家安全教育	1	16	16	0	1								考查	马院
		必修	实验室安全教育	1	16	16	0		1							考查	计智学院
		必修	体育Ⅰ	1	36	12	24	1								考查	人文学院
		必修	体育Ⅱ	1	36	8	28		1							考查	人文学院
		必修	体育Ⅲ	1	36	8	28			1						考查	人文学院
		必修	体育Ⅳ	1	36	8	28				1					考查	人文学院
		小计		**10**	**244**	**120**	**124**	**4**	**4**	**1**	**1**	**0**	**0**	**0**	**0**		
	创新创业模块	**必修**	创业基础	2	32	16	16				2					考查	马院
		必修	职业生涯规划与就业指导	2	32	16	16	2								考查	马院
		小计		**4**	**64**	**32**	**32**	**2**	**0**	**0**	**2**	**0**	**0**	**0**	**0**		
	通识素养模块	**必修**	社会公益1	1	16	16	0		1							考查	马院/社院
		必修	社会公益2	1	16	16	0				1					考查	马院/社院
		必修	美育教育1	0.5	8	8	0	0.5								考查	艺传学院
		必修	美育教育2	0.5	8	8	0					0.5				考查	艺传学院
		必修	公共艺术（史论类）	0.5	8	8	0			0.5						考查	艺传学院
		必修	公共艺术（鉴赏评论类）	0.5	8	8	0				0.5					考查	艺传学院
		必修	AI入门	1	16	16	0			1						考查	计智学院
		选修	公共选修课	2	32	32	0								2	考查	各学院
		必修	写作与沟通课程A	2	32	24	8			2						考查	经管学院
		小计		**9**	**144**	**136**	**8**	**0.5**	**1**	**3.5**	**1.5**	**0.5**	**0**	**0**	**2**		
	合计			**53**	**964**	**696**	**268**	**13**	**12.5**	**11**	**14**	**0.5**	**0**	**0**	**2**		
专	**学科**	**必修**	高等数学(Ⅰ)	4	64	64	0	4								考试	计智学院

业教育平台	（专业）基础课模块	**必修**	高等数学（II）	5	80	80	0		5							考试	计智学院
		必修	线性代数	3	48	48	0		3							考试	计智学院
		必修	概率论与数理统计	2.5	40	40	0			2.5						考试	计智学院
		必修	离散数学	2.5	40	40	0			2.5						考试	计智学院
		必修	数字逻辑	2	32	24	8		2							考试	计智学院
		必修	C语言程序设计	4	64	48	16	4								考试	计智学院
		必修	计算机网络	3	48	32	16		3							考试	计智学院
		必修	数据结构与算法分析	4	64	48	16		4							考试	计智学院
		小计		**30**	**480**	**424**	**56**	**8**	**17**	**5**	**0**	**0**	**0**	**0**	**0**		
	专业核心课模块	**必修**	计算机组成原理	3	48	40	8			3						考试	计智学院
		必修	数据库原理及应用	3	48	32	16				3					考试	计智学院
		必修	操作系统原理	3	48	32	16				3					考试	计智学院
		必修	网络空间安全导论	3	48	32	16			3						考试	计智学院
		必修	通信原理	3	48	32	16			3						考试	计智学院
		必修	计算机网络安全	3	48	32	16				3					考试	计智学院
		必修	密码学基础	3	48	32	16				3					考查	计智学院
		必修	软件安全与逆向分析	3	48	32	16					3				考查	计智学院
		必修	操作系统安全	3	48	32	16					3				考查	计智学院
		必修	网络攻防与渗透测试	3	48	32	16						3			考查	计智学院
		必修	Web安全技术	3	48	32	16						3			考查	计智学院
		小计		**33**	**528**	**360**	**168**	**0**	**0**	**9**	**12**	**6**	**6**	**0**	**0**		

	专业选修（拓展）课模块	**选修**	物联网通信技术	2	32	24	8		2							考查	计智学院
		选修	无线传感网络	2	32	24	8		2							考查	计智学院
		选修	云计算	2	32	24	8			2						考查	计智学院
		选修	数据采集与处理	2	32	24	8			2						考查	计智学院
		选修	大数据技术	2	32	24	8				2					考查	计智学院
		选修	人工智能技术应用	2	32	24	8				2					考查	计智学院
		选修	现代通信技术	2	32	24	8					2				考查	计智学院
		选修	数字信号处理	2	32	24	8					2				考查	计智学院
		选修	智能网联汽车技术	2	32	24	8						2			考查	计智学院
		选修	移动APP设计与开发	2	32	24	8						2			考查	计智学院
		选修	Python程序设计	2	32	24	8		2							考查	计智学院
		选修	Java程序设计	2	32	24	8		2							考查	计智学院
		选修	智能终端软件开发	2	32	24	8			2						考查	计智学院
		选修	Java web开发技术							2						考查	计智学院
		选修	软件工程	2	32	24	8				2					考查	计智学院
		选修	软件测试技术	2	32	24	8				2					考查	计智学院
		选修	机器学习与实践	2	32	24	8					2				考查	计智学院
		选修	电子系统设计	2	32	24	8					2				考查	计智学院
		选修	智能控制	2	32	24	8						2			考查	计智学院
		选修	智能硬件设计与实践	2	32	24	8						2			考查	计智学院
		小计（最低选修20学分）		**20**	**320**	**240**	**80**	**0**	**4**	**4**	**4**	**4**	**4**	**0**	**0**		
	合计（最低选修20学分）			**83**	**1328**	**1024**	**304**	**8**	**21**	**18**	**16**	**10**	**10**	**0**	**0**		

实践教学平台	通识实践模块	**必修**	军事技能	2	2W	0	2W	2								考查	马院/学工
		必修	劳动教育(含劳动理论)	2	2W	0	2W		2							考查	马院/学工
		小计		**4**	**4W**	**0**	**4W**	**2**	**2**	**0**	**0**	**0**	**0**	**0**	**0**		
		必修	AI大模型应用（训练营）	2	2W	0	2W				2					考查	
		必修	C语言课程设计	1	1W		1W		1							考查	计智学院
		必修	网络空间安全工程与应用	1	1W	0	1W			1						考查	计智学院
		必修	网络安全技术及综合实践	2	2W	0	2W					2				考查	计智学院
		必修	专业综合实训（产教融合）	2	2W	0	2W					2				考查	计智学院
		必修	生产实习（产教融合）	2	2W	0	2W						2			考查	计智学院
		必修	毕业实习	10	20W	0	20W							10		考查	计智学院
		必修	毕业设计（论文）	6	6W	0	6W								6	考查	计智学院
		小计		**26**	**36W**	**0**	**36W**	**0**	**1**	**1**	**2**	**4**	**2**	**10**	**6**		
	合计			**30**	**40W**	**0**	**40W**	**2**	**3**	**1**	**2**	**4**	**2**	**10**	**6**		
个性化发展平	**选修**		国内考研	4	4W	0	4W									考查	计智学院
	选修		学科竞赛	4	4W	0	4W									考查	计智学院
	选修		学术讲座	1	1W	0	1W									考查	计智学院
	选修		职业技能证书	2	2W	0	2W									考查	计智学院

台	**选修**	专业服务实践	3	3W	0	3W									考查	计智学院
	小计（最低选修4学分）		**4**	**4W**	**0**	**4W**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**4**	此平台学分计入第八学期	
	合计		**4**	**4W**	**0**	**4W**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**4**	此平台学分计入第八学期	
全球化教育平台	**选修**	海外教育概况	2	32	32	0									考查	国教学院
	选修	微留学项目	2	32	0	32									考查	国教学院
	选修	跨文化交流	2	32	32	0									考查	国教学院
	选修	中外文化比较	2	32	32	0									考查	国教学院
	此平台学分不计入毕业要求学分															
总计			**170**	**2292+44W**	**1720**	**572+44W**	**23**	**36.5**	**30**	**32**	**14.5**	**12**	**10**	**12**		

十、毕业要求对培养目标的支撑关系

毕业要求与培养目标对应关系表

培养目标 毕业要求	培养目标1	培养目标2	培养目标3
毕业要求1			√
毕业要求2	√		
毕业要求3		√	
毕业要求4		√	
毕业要求5			√
毕业要求6			√

十一、课程体系对毕业要求的支撑关系

课程体系对毕业要求的支撑关系表

课程类型		课程属性	课程名称	毕业要求																
				毕业要求1				毕业要求2				毕业要求3			毕业要求4		毕业要求5		毕业要求6	
				1-1	1-2	1-3	1-4	2-1	2-2	2-3	2-4	3-1	3-2	3-3	4-1	4-2	5-1	5-2	6-1	6-2
通识教育平台	思政课模块	必修	思想道德与法治	√																
		必修	中国近现代史纲要		√															
		必修	马克思主义基本原理			√														
		必修	毛泽东思想和中国特色社会主义理论体系概论				√													
		必修	习近平新时代中国特色社会主义思想概论	√																
		选修	“四史”课程		√															
		必修	形势与政策			√														
	语言课模块	必修	大学英语Ⅰ														√			
		必修	大学英语Ⅱ															√		
		必修	大学英语Ⅲ														√			
		必修	大学英语Ⅳ															√		
	身心健康模块	必修	军事理论	√																
		必修	大学生心理健康		√															
		必修	国家安全教育			√														
		必修	实验室安全教育			√														
		必修	体育Ⅰ																	
		必修	体育Ⅱ																	
		必修	体育Ⅲ																	
		必修	体育Ⅳ																	
	创新创业模块	必修	创业基础				√													
		必修	职业生涯规划与就业指导																√	
	通识	必修	AI入门																	√

	素养模块	必修	美育教育1	√																
		必修	美育教育2		√															
		必修	公共艺术（史论类）	√																
		必修	公共艺术（鉴赏评论类）		√															
		必修	公共选修课				√													
		必修	写作与沟通课程A														√			
		必修	社会公益1					√												
		必修	社会公益2						√											
专业教育平台	学科（专业）基础课模块	必修	高等数学(I)									√								
		必修	高等数学(II)									√								
		必修	线性代数										√							
		必修	概率论与数理统计										√							
		必修	离散数学											√						
		必修	数字逻辑									√								
		必修	C语言程序设计										√							
		必修	计算机网络											√						
		必修	数据结构与算法分析									√								
	专业核心课模块	必修	计算机组成原理										√							
		必修	数据库原理及应用											√						
		必修	操作系统原理									√								
		必修	网络空间安全导论										√							
		必修	通信原理											√						
		必修	计算机网络安全									√								
		必修	密码学基础										√							
		必修	软件安全与逆向分析											√						
		必修	操作系统安全									√								
		必修	网络攻防与渗透测试										√							
		必修	Web安全技术											√						
	专业选修、专业拓展	选修	物联网通信技术					√												
		选修	无线传感器网络						√											
		选修	云计算							√										
		选修	数据采集与处理								√									

	（方向）课模块	选修	大数据技术									√								
		选修	人工智能技术应用										√							
		选修	现代通信技术											√						
		选修	数字信号处理					√												
		选修	智能网联汽车技术						√											
		选修	移动APP设计与开发							√										
		选修	Python程序设计								√									
		选修	Java程序设计									√								
		选修	智能终端软件开发										√							
		选修	Java web开发技术											√						
		选修	软件工程					√												
		选修	软件测试技术						√											
		选修	机器学习与实践							√										
		选修	电子系统设计								√									
		选修	智能控制									√								
		选修	智能硬件设计与实践										√							
实践教学平台	通识实践模块	必修	军事技能	√																
		必修	劳动教育(含劳动理论)		√															
	专业实践模块	必修	AI大模型应用（训练营）																√	√
		必修	网络空间安全工程与应用										√							
		必修	C语言课程设计										√							
		必修	网络安全技术及综合实践							√										
		必修	专业综合实训（产教融合）											√						
		必修	生产实习（产教融合）											√						
		必修	毕业实习											√						
		必修	毕业设计（论文）							√										
个性	选修		国内考研																√	

化发展平台	选修	学科竞赛													√				
	选修	学术讲座																√	
	选修	职业技能证书																	√
	选修	专业实践服务								√									

十三、教学进程计划表（附表）

课程类型		课程属性	课程名称	学分	学时	学时分类		学期	备注
						讲课	实践		
通识教育平台	思政课模块	必修	思想道德与法治	3	48	40	8	1	
		必修	中国近现代史纲要	3	48	40	8	2	
		必修	马克思主义基本原理	3	48	40	8	3	
		必修	毛泽东思想和中国特色社会主义理论体系概论	3	48	40	8	4	
		必修	习近平新时代中国特色社会主义思想概论	3	48	40	8	4	
		选修	“四史”课程	1	16	16	0	2	
		必修	形势与政策	2	64	64	0		
		小计		**18**	**320**	**280**	**40**		
	语言课模块	必修	大学英语I	3	48	32	16	1	
		必修	大学英语II	3	48	32	16	2	
		必修	大学英语III	3	48	32	16	3	
		必修	大学英语IV	3	48	32	16	4	
		小计		**12**	**192**	**128**	**64**		
	身心健康模块	必修	军事理论	2	36	36	0	1	
		必修	大学生心理健康	2	32	16	16	2	
		必修	国家安全教育	1	16	16	0	1	
		必修	实验室安全教育	1	16	16	0	2	
		必修	体育I	1	36	12	24	1	
		必修	体育II	1	36	8	28	2	
		必修	体育III	1	36	8	28	3	
		必修	体育IV	1	36	8	28	4	
		小计		**9**	**228**	**104**	**124**		
	创新创业模块	必修	创业基础	2	32	16	16	4	
		必修	职业生涯规划与就业指导	2	32	16	16	1	
		小计		**4**	**64**	**32**	**32**		
	通识素养模块	必修	AI入门	1	16	16	0	1	
		必修	美育教育1	0.5	8	8	0	1	
		必修	美育教育1	0.5	8	8	0	5	
		必修	公共艺术（史论类）	0.5	8	8	0	2	
		必修	公共艺术（鉴赏评论类）	0.5	8	8	0	3	
		选修	公共选修课	2	32	32	0		
		必修	写作与沟通课程A	2	32	24	8	3	
		必修	社会公益1	1	16	0	16	2	
		必修	社会公益2	1	16	0	16	4	
		小计		**9**	**144**	**136**	**8**		
	合计			**53**	**964**	**696**	**268**		
专业教育平台	学科（专业）基础课模块	必修	高等数学(I)	4	64	64	0	1	
		必修	高等数学(II)	5	80	80	0	2	
		必修	线性代数	3	48	48	0	2	
		必修	概率论与数理统计	2.5	40	40	0	3	
		必修	离散数学	2.5	40	40	0	3	
		必修	数字逻辑	2	32	24	8	2	
		必修	C语言程序设计	4	64	48	16	1	
		必修	计算机网络	3	48	32	16	2	

		必修	数据结构与算法分析	4	64	48	16	2	
		小计		**30**	**480**	**424**	**56**		
	专业核心课模块	**必修**	计算机组成原理	3	48	40	8	3	
		必修	数据库原理及应用	3	48	32	16	4	
		必修	操作系统原理	3	48	32	16	4	
		必修	网络空间安全导论	3	48	32	16	3	
		必修	通信原理	3	48	32	16	3	
		必修	计算机网络安全	3	48	32	16	4	
		必修	密码学基础	3	48	32	16	4	
		必修	软件安全与逆向分析	3	48	32	16	5	
		必修	操作系统安全	3	48	32	16	5	
		必修	网络攻防与渗透测试	3	48	32	16	6	
		必修	Web安全技术	3	48	32	16	6	
		小计		**33**	**528**	**360**	**168**		
	专业选修（拓展）课模块	**选修**	物联网通信技术	2	32	24	8	2	
		选修	无线传感网络	2	32	24	8	2	
		选修	云计算	2	32	24	8	3	
		选修	数据采集与处理	2	32	24	8	3	
		选修	大数据技术	2	32	24	8	4	
		选修	人工智能技术应用	2	32	24	8	4	
		选修	现代通信技术	2	32	24	8	5	
		选修	数字信号处理	2	32	24	8	5	
		选修	智能网联汽车技术	2	32	24	8	6	
		选修	移动APP设计与开发	2	32	24	8	6	
		选修	Python程序设计	2	32	24	8	2	
		选修	Java程序设计	2	32	24	8	2	
		选修	智能终端软件开发	2	32	24	8	3	
		选修	Java web开发技术	2	32	24	8	3	
		选修	软件工程	2	32	24	8	4	
		选修	软件测试技术	2	32	24	8	4	
		选修	机器学习与实践	2	32	24	8	5	
		选修	电子系统设计	2	32	24	8	5	
		选修	智能控制	2	32	24	8	6	
		选修	智能硬件设计与实践	2	32	24	8	6	
		小计（最低选修20学分）		**20**	**320**	**240**	**80**		
	合计（最低选修20学分）			**83**	**1328**	**1024**	**304**		
实践教学平台	**通识实践模块**	**必修**	军事技能	2	2W	0	2W	1	
		必修	劳动教育(含劳动理论)	2	2W	0	2W	2	
		小计		**4**	**4W**	**0**	**4W**		
	专业实践模块	**必修**	AI大模型应用(训练营)	2	2W	0	2W	4	
		必修	C语言课程设计	1	1W	0	1W	2	
			网络空间安全工程与应用	1	1W	0	1W	3	
		必修	网络安全技术及综合实践	2	2W	0	2W	5	
		必修	专业综合实训（产教融合）	2	2W	0	2W	5	
		必修	生产实习（产教融合）	2	2W	0	2W	6	
		必修	毕业实习	10	20W	0	20W	7	
		必修	毕业设计（论文）	6	6W	0	6W	8	
		小计		**26**	**36W**	**0**	**36W**		
	合计			**30**	**40W**	**0**	**40W**		

个性化发展平台	**选修**	国内考研	4	4W	0	4W	此平台学分计入第八学期	
	选修	学科竞赛	4	4W	0	4W		
	选修	学术讲座	1	1W	0	1W		
	选修	职业技能证书	2	2W	0	2W		
	选修	专业实践服务	3	3W	0	3W		
	小计（最低选修4学分）		**4**	**4W**	**0**	**4W**		
全球化教育平台	**选修**	海外教育概况	2	32	32	0		
	选修	微留学项目	2	32	0	32		
	选修	跨文化交流	2	32	32	0		
	选修	中外文化比较	2	32	32	0		
	此平台不计入毕业学分要求							
总计			**170**	**2292+44W**	**1720**	**572+44W**		

培养方案制定人：

培养方案审核人

培养方案批准人：

6. 教师及课程基本情况表

6.1专业核心课程情况表

课程名称	课程总学时	课程周学时	拟授课教师	授课学期
计算机组成原理	48	3	黎丽	3
网络空间安全导论	48	3	宋军	3
通信原理	48	3	叶雪军	3
数据库原理及应用	48	3	吴蓓	4
操作系统原理	48	3	王金庭	4
计算机网络安全	48	3	李向	4
密码学基础	48	3	陈宇	4
软件安全与逆向分析	48	3	刘艳	5
操作系统安全	48	3	冯春华	5
网络攻防与渗透测试	48	3	晏轲	6
Web安全技术	48	3	蔡之华	6

6.2本专业授课教师基本情况表

姓名	性别	出生年月	拟授课程	专业技术职务	学历	最后学历毕业学校	最后学历毕业专业	最后学历毕业学位	研究领域	专职/兼职
宋军	男	1974-03	网络空间安全导论	教授	研究生	武汉大学	计算机软件与理论	博士	密码学及应用、无线网络安全	专职
蔡之华	男	1963-04	Web安全技术	教授	研究生	中国地质大学（武汉）	地球探测与信息技术	博士	机器学习、演化算法	专职
童恒建	男	1971-11	网络攻防与渗透测试	教授	研究生	中国地质大学（武汉）	地理信息系统	博士	遥感图像处理与分析	专职
黎丽	女	1982-10	计算机组成原理	教授	研究生	华中科技大学	凝聚态物理	博士	分形理论与应用、复杂网络	专职
刘艳	女	1980-04	软件安全	教授	研究生	中国地质	计算机应	硕士	计算机应	专职

			与逆向分析			大学（武汉）	用技术		用	
李星	男	1962-06	离散数学	教授	研究生	中国地质大学（武汉）	矿产普查与勘探	博士	计算机应用	专职
李向	男	1970-09	计算机网络安全	副教授	研究生	中国地质大学（武汉）	地学信息工程	博士	智能计算与目标检测	专职
晏轲	女	1983-11	网络攻防与渗透测试	副教授	研究生	华中科技大学	计算机科学与技术	博士	计算机应用	专职
陈宇	女	1982-09	密码学基础	副教授	研究生	华中科技大学	计算机应用技术	硕士	信息安全	专职
邵玉祥	男	1971-03	数据结构与算法分析	副教授	研究生	武汉理工大学	计算机应用技术	博士	计算机应用	专职
冯春华	女	1982-04	操作系统安全	副教授	研究生	华东交通大学	电力系统及其自动化	硕士	计算机应用	专职
吴蓓	女	1982-07	数据库原理及应用	副教授	研究生	华中师范大学	教育技术学	硕士	计算机应用	专职
徐梅	女	1979-10	C语言程序设计	副教授	研究生	湖北大学	系统分析与集成	硕士	软件开发	专职
望超	男	1990-03	无线传感网络	讲师	研究生	中国地质大学（武汉）	电子与通信工程	硕士	嵌入式技术	专职
王金庭	男	1976-12	操作系统原理	副教授	研究生	中国地质大学（武汉）	计算机应用技术	硕士	人工智能	专职
叶雪军	女	1976-08	通信原理	副教授	研究生	华中科技大学	通信与信息系统	硕士	通信技术	专职
鲜军	男	1973-07	Java程序设计	副教授	研究生	武汉大学	软件工程	硕士	软件开发	专职
成晓利	男	1986-09	网络安全技术及综合实践	其他中级	研究生	西南交通大学	信息安全	硕士	信息安全	专职

6.3教师及开课情况汇总表

专任教师总数	18		
具有教授（含其他正高级）职称教师数	6	比例	33.33%
具有副教授及以上（含其他副高级）职称教师数	16	比例	88.89%
具有硕士及以上学位教师数	18	比例	100.00%
具有博士学位教师数	8	比例	44.44%
35岁及以下青年教师数	1	比例	05.56%
36-55岁教师数	15	比例	83.33%
兼职/专职教师比例	0:18		
专业核心课程门数	11		
专业核心课程任课教师数	11		

7. 专业主要带头人简介

姓名	李向	性别	男	专业技术职务	副教授	行政职务	无
拟承担课程	计算机网络安全、Java程序设计			现在所在单位	武汉工程科技学院		
最后学历毕业时间、学校、专业		博士研究生、2008年7月毕业于中国地质大学（武汉），地学信息工程					
主要研究方向		智能计算与目标检测					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		发表T4及以上论文6篇，CCF-C论文2篇，教学研究论文3篇					
从事科学研究及获奖情况		2011年获优秀测绘工程奖,银奖,四川省绵竹至茂县公路工程测量,排名11,中国测绘学会; 2011年获“2011年度市引进国外经济技术专家项目工作贡献奖”,武汉市外国专家局; 2012年获,优秀测绘工程奖一等奖,新疆喀什至伊尔克什坦高速公路工程测量,排名5,中国测绘学会; 2012年获地理信息科技进步奖二等奖,基于LiDAR技术的道路智能设计方法及系统研究,排名5,国家测绘地理信息局; 2014获地理信息科技进步奖二等奖,真三维可视化公路建设项目管理关键技术研究与应用,排名2,中国地理信息产业协会; 2016年获地理信息科技进步奖三等奖,真三维高速公路运营智能管理技术研究,排名6,中国地理信息产业协会。					
近三年获得教学研究经费（万元）	5.0			近三年获得科学研究经费（万元）	43.0		
近三年给本科生授课课程及学时数	授课计算机网络学时48，Java程序设计学时48			近三年指导本科毕业设计（人次）	24		

姓名	刘艳	性别	女	专业技术职务	教授	行政职务	系主任

<table>
<tr><td>拟承担课程</td><td colspan="3">数据结构与算法分析、操作系统</td><td>现在所在单位</td><td colspan="3">武汉工程科技学院</td></tr>
<tr><td colspan="2">最后学历毕业时间、学校、专业</td><td colspan="6">硕士研究生、2007年毕业于中国地质大学（武汉）、计算机应用技术</td></tr>
<tr><td colspan="2">主要研究方向</td><td colspan="6">计算机应用</td></tr>
<tr><td colspan="2">从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）</td><td colspan="6">2025年获批湖北省教育厅新工科实践教学项目1项；2024年获批全国高等院校计算机基础教育研究会项目1项；近三年主持获批教育部协同育人项目3项；2020-2024年出版教材5部。</td></tr>
<tr><td colspan="2">从事科学研究及获奖情况</td><td colspan="6">主持完成湖北省教育厅科学技术研究计划指导性项目1项</td></tr>
<tr><td>近三年获得教学研究经费（万元）</td><td colspan="3">5.5</td><td>近三年获得科学研究经费（万元）</td><td colspan="3">2.0</td></tr>
<tr><td>近三年给本科生授课课程及学时数</td><td colspan="3">授课数据结构与算法分析学时64，虚拟现实开发学时48；Python程序设计学时48，图形图像原理学时32</td><td>近三年指导本科毕业设计（人次）</td><td colspan="3">13</td></tr>
<tr><td>姓名</td><td>黎丽</td><td>性别</td><td>女</td><td>专业技术职务</td><td>教授</td><td>行政职务</td><td>教学副院长</td></tr>
<tr><td>拟承担课程</td><td colspan="3">计算机组成原理、通讯原理</td><td>现在所在单位</td><td colspan="3">武汉工程科技学院</td></tr>
<tr><td colspan="2">最后学历毕业时间、学校、专业</td><td colspan="6">博士研究生、2014年6月毕业于华中科技大学、凝聚态物理</td></tr>
<tr><td colspan="2">主要研究方向</td><td colspan="6">分形理论与应用、 复杂网络</td></tr>
<tr><td colspan="2">从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）</td><td colspan="6">2019年主持获批湖北高校省级教学团队：计算机系列课程教学团队；2020年主持获批湖北高校省级一流专业建设点：计算机科学与技术专业；2021年参与（序2）获批湖北省级一流课程（操作系统）；近几年主持参与教育部协同育人项目7项。</td></tr>
<tr><td colspan="2">从事科学研究及获奖情况</td><td colspan="6">主持完成湖北省教育科学“十二五”规划课题1项、湖北省教育厅科学研究计划项目1项；2024年主持获批北省教育厅科学研究计划项目1项。</td></tr>
<tr><td>近三年获得教学研究经费（万元）</td><td colspan="3">3.0</td><td>近三年获得科学研究经费（万元）</td><td colspan="3">4.0</td></tr>
<tr><td>近三年给本</td><td colspan="3">授课计算机组成原理学时56；数字逻</td><td>近三年指导</td><td colspan="3">14</td></tr>
</table>

科生授课课程及学时数	辑学时40	本科毕业设计（人次）	

姓名	蔡之华	性别	男	专业技术职务	教授	行政职务	院长
拟承担课程	Web安全技术、离散数学			现在所在单位	武汉工程科技学院		
最后学历毕业时间、学校、专业		博士研究生、2003年7月毕业于中国地质大学（武汉）、地球探测与信息技术					
主要研究方向		机器学习、演化算法					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		主持的教研项目获2013年及2022年湖北省教学成果二等奖各一次，2023年主持完成湖北省教研项目1项					
从事科学研究及获奖情况		主持的项目2014年获湖北省自然科学二等奖；参与的（序3）项目2021年获湖北省自然科学二等奖					
近三年获得教学研究经费（万元）	5.0			近三年获得科学研究经费（万元）	40.0		
近三年给本科生授课课程及学时数	授课离散数学课程学时48			近三年指导本科毕业设计（人次）	12		

姓名	宋军	性别	男	专业技术职务	教授	行政职务	无
拟承担课程	网络空间安全导论、密码学基础			现在所在单位	武汉工程科技学院		
最后学历毕业时间、学校、专业		博士研究生、2008年7月毕业于武汉大学、计算机软件与理论					
主要研究方向		无线网络安全、大数据安全					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		2018年获湖北省教学成果二等奖；五次荣获全国大学生科技竞赛优秀指导教师					
从事科学研究及获奖情况		在重要期刊和国际会议上发表SCI科研论文20余篇，获得国家发明专利26项					

近三年获得教学研究经费（万元）	20.0	近三年获得科学研究经费（万元）	130.0
近三年给本科生授课课程及学时数	授课网络空间安全导论课程学时40；授课C语言程序设计课程64学时	近三年指导本科毕业设计（人次）	16

8. 教学条件情况表

可用于该专业的教学实验设备总价值（万元）	955.47	可用于该专业的教学实验设备数量（千元以上）	1086（台/件）
开办经费及来源	（1）民办高校自筹经费。武汉工程科技大学作为民办高校，具备灵活的经费调配机制。举办者将通过资金投入保障新专业建设，同时积极争取社会捐赠和校友基金支持，用于改善办学条件、提升专业建设水平。 （2）校级专业建设专项经费。学校在年度预算中设立专项经费用于重点支持新专业建设，专项经费将优先用于网络空间安全专业的课程开发、师资引进、实验平台建设等环节。 （3）专项实验室建设经费。学校设有实验室建设专项经费，来源包括校本投入和项目单位配套资金。网络空间安全专业实验室建设将依托计算机与人工智能学院已有实验资源，结合新购软硬件系统进行升级扩展。 （4）校企合作专项支持。依托现有校企合作基础，学校将积极申报教育部产教融合项目，推动与安全企业、数据服务商、运营商的合作，通过联合建设实训基地、共建课程项目等方式引入企业资金。 （5）社会服务与项目收入。通过科研课题、企业委托开发、技术服务等项目所获得经费将持续反哺专业发展，增强资金持续保障能力。		
生均年教学日常运行支出（元）	1568.0		
实践教学基地（个）	9		
教学条件建设规划及保障措施	（1）优化师资队伍结构。学校将依托计算机与人工智能学院现有教学资源，统筹规划网络空间安全专业师资队伍建设，计划引进具有信息安全、密码学、网络攻防等方向的博士及高职称人才2-3名，培育1-2名专业带头人；遴选骨干教师赴知名高校访学或产业实践，提升教学与工程实践能力，构建“专兼结合、产教融合”的教学团队。 （2）建设专业特色实验平台。依托现有计算机科学与技术、软件工程、信息安全技术等实验基础，建设包括攻防对抗实验平台、网络取证平台、漏洞分析平台等在内的网络安全综合实验环境。 （3）推进产教融合实践教学。拓展校外实训基地，强化与安全厂商、公安系统、信息安全服务企业的合作，推行项目式、案例式教学。 （4）创新教学组织模式。推动“课程-项目-竞赛-实训”一体化教学体系，积极组织学生参与网络安全大赛等高水平竞赛，实现“以赛促学、以赛促教、以赛促建”；推进智慧教学平台建设，提升教学信息化水平，打造具有工科特色的复合型人才培养环境。		

主要教学实验设备情况表

教学实验设备名称	型号规格	数量	购入时间	设备价值（千元）
安恒明御攻防实验平台	DELL服务器2、CPU-E5-2620内存-128GB硬盘-4T Raid 512M缓存网口：千兆*4	1	2023	45.6
硬件VPN网关	万兆防火墙级VPN专用网关	1	2022	25.0
安全隔离与信息交换系统	内外网数据单向导入隔离网闸	1	2022	35.0
网络密码机	高速网络加密设备，支持国密算法	1	2022	30.0
二层交换机	Cisco Catalyst 2950	35	2018	25.0
路由器	Cisco 2621	35	2018	35.0
三层核心交换机	星网锐捷 RG系列	35	2018	87.5
路由器	星网锐捷 RG系列	35	2018	105.0
无线接入器（AP）	TP-Link/华为企业级AP	35	2019	122.5
计算机组成原理实验箱	清华科教 TEC5AH	35	2019	105.0
微机接口实验箱	清华科教 TPC-USB+	80	2022	42.0
虚拟化实验服务器	Dell PowerEdge R730	40	2022	70.0
网络过滤网关设备	KILL KSG-5000	1	2022	200.0
VPN软件系统	山石网科或深信服VPN平台软件	1	2022	80.0
网络防病毒软件	企业级终端安全系统（如Symantec或360天擎）	1	2022	50.0
漏洞扫描系统	绿盟或安恒Web漏洞扫描平台	1	2023	100.0
网络协议仿真软件	GNS3/Packet Tracer	1	2023	20.0
网络协议分析软件	Wireshark企业授权	1	2024	10.0

	版			
网络攻防实验平台软件	安恒明御网络攻防演练平台	1	2024	200.0
网络取证分析系统	联软/启明星辰日志审计与网络取证系统	1	2024	150.0
数字电路实验箱	LMT-SZ-IV型	35	2022	70.0
惠普分体式电脑	HP Z2 G5 TWR+E27q	120	2022	1574.4
电路分析基础实验箱	LMTDL-V型	35	2018	52.2
直流稳压电源	YB1732A\2A	35	2018	35.0
嵌入式Cortex-A9高级教学系统	博嵌BQA9-6	30	2022	238.5
EDA技术实验箱	EP4C10	35	2018	105.0
DSP技术实验箱	HK-EP	35	2018	122.5
万能单片机实验开发系统	DJ-52EH+	35	2022	137.55
RFID教学实验箱	FS-RFID	20	2022	180.0
物联网综合实验箱	FSWSN6818CP	20	2022	340.0
AI智能家居实训套件	FS-AIVRJJ	4	2022	120.0
AI智慧城市综合实训系统	FS-ICS	1	2022	280.0
智慧实训管理平台	NGT-ITMP	1	2022	400.0
NEC投影仪	NP-PE523X+	1	2022	17.78
美叶幕布	150寸4:3	1	2022	1.1
快思捷中央控制器	VS-IV	1	2022	1.23
NEC投影仪	NP-PE523X+	2	2022	35.56
美叶幕布	150寸4:3	2	2022	2.2
快思捷中央控制器	VS-IV	2	2022	2.46
云管理服务器	锐捷RG-RCD6000 V4	1	2019	60.0
云教学管理软件	锐捷License70	1	2019	3.9
云终端（教师端）	锐捷RG-Rain310E(500HD)	1	2019	3.9
云终端（学生端）	锐捷RG-Rain100 V2	40	2019	49.6
不间断电源UPS	深圳山特RACK	1	2020	13.5

	10KS（含导轨）			
IDV服务器	RG-CS1020、RG-CCP-DCP-Lic-EDU	4	2022	150.4
计算服务器	H3C R4900 G3	4	2022	151.92
管理服务器	H3C R4900 G3	1	2022	23.96
惠普分体式电脑	HP Z2 G5 TWR+E27q	80	2023	1049.6
NEC投影仪	NP-PE523X+	1	2023	17.78
美叶幕布	150寸4:3	1	2023	1.1
快思捷中央控制器	VS-IV	1	2023	1.23
工业机器人多功能实训工作站	NGT-RA6X	4	2022	1200.0
工业机器人装调应用与维护实训平台	NGT-RTW01	4	2022	1000.0
电子焊接实训台	HC1E0AB	80	2022	160.0
模拟电路实验箱	BQ/MI-6	35	2022	91.0
示波器	NDS102	35	2022	185.5
任意信号发生器	WT3360X	35	2022	138.25

9. 申请增设专业的理由和基础

武汉工程科技学院增设网络空间安全本科专业的必要性与可行性论证报告

一、增设专业的主要理由

1. 国家战略和政策驱动

网络空间安全已上升为国家战略高度。党和政府高度重视网络安全人才培养，近年来相继出台《国家网络空间安全战略》[1]、《关于增设网络空间安全一级学科的通知》[2]、《关于加强网络安全学科建设和人才培养的意见》[3]、《中华人民共和国网络安全法》[4]以及《“十四五”国家信息化规划》[5]等一系列政策规划。这些顶层设计明确要求加快网络安全学科建设，强化网络安全人才培养，以支撑国家安全和数字经济发展需求。其中，《“十四五”数字经济发展规划》[6]强调要“加强网络安全宣传教育和人才培养”。增设网络空间安全本科专业正是响应国家战略需求，对接政策导向，为“网络强国”战略提供人才支撑的重要举措。

2. 网络安全产业发展与人才需求

当前信息技术与网络攻击手段日益演进，网络空间已被视为继陆、海、空、天之后的“第五空间”[7]。网络安全产业规模正持续高速扩张，新技术、新业态层出不穷，催生海量专业人才需求。据统计，“十四五”期间我国信息安全行业加速重构升级，市场规模快速扩大，急需大量具备实践能力的网络安全专业人才，而现有本科层次人才培养供给明显不足[8]。网络安全已成为高薪领域，人才价值凸显——麦可思《中国本科生就业报告（2024）》[9]显示，信息安全专业毕业生平均薪资已连续五年位居工科本科首位。然而人才供给远未满足市场需求：教育部预测到2027年我国网络安全人员缺口将达327万人，而高校相关专业年培养规模仅约3万人[10]。网络安全人才短缺已成为制约产业发展的突出瓶颈，亟需高校扩大培养规模、提升培养质量。设立本专业可为国家战略新兴产业输送急需的高素质网络安全工程师，满足蓬勃的行业人才需求[15]。

3. 区域发展态势与岗位需求

武汉作为中部地区的重要科教基地，拥有丰富的高校和科研资源，在发展网络安全教育方面具备独特优势[11]。目前国家网络安全人才与创新基地落户武汉，“武汉网络空间安全学院”等项目正在建设，将集聚大批创新资源和人才[11]。同时，湖北省信息化建设提速，全行业对具备本科学历和专业技能的网络安全人才产生迫切需求[12]。湖北省内网络与信息安全企业众多且处于成长期，对网络安全人才的需求尤为旺盛[12]。据调研统计，湖北省网络安全岗位对3-5年经验人才的招聘占比达65%，其中大专及以上学历需求约占58%[12]。本科层次网络安全人才在武汉及周边新兴城市拥有旺盛的就业机会和广阔发展空间。我校增设该专业，既可发挥区位和资源优势培养本地人才，又能反哺区域数字经济和网络安全产业的发展，实现高校服务区域发展的使命。

4. 高校教育供需矛盾

目前全国开设“网络空间安全”本科专业的高校数量相对有限。截至2025年6月，全国已有143所高校获批设立网络空间安全本科专业[13]。在湖北省，虽有武汉大学、华中科技大学等高校涉足信息安全相关领域，但本科层次布局仍有提升空间，许多院校主要在高职阶段开设相关专业[14]。人才培养供给与社会需求间存在明显矛盾：一方面行业“求才若渴”，另一方面本科教育产出的人才数量不足且结构不够完善，特别是应用型本科人才供给短缺[14]。作为应用型本科高校，此时申办网络空间安全本科专业正当其时，可有效填补区域本科人才培养空白。这既是顺应教育供给侧改革、优化学科专业布局的需要，也是缓解网络安全人才供需矛盾的积极举措。

综上，增设网络空间安全本科专业具有坚实的背景理由：上承国家战略要求，下应产业和区域发展需求，中解教育供给不足之急。该专业的设置对于强化国家网络安全人才储备、服务地方经济和保障网络空间安全都具有重要意义和迫切性。

二、支撑专业发展的学科基础

1. 相关学科专业基础

我校计算机学科经过多年建设，已形成坚实基础并积累了丰富经验，构建起计算机类人才培养的完整体系，为新专业建设奠定了良好基础。学院始终紧扣“地方性、应用型”的办学定位，注重学生实践能力培养，在专业建设上硬件条件达标、教学秩序优良、产学研合作深入。依托现有计算机类专业的课程体系、教材资源和教学平台，新专业在课程设置和知识衔接上有充足支撑。总体而言，我校

在计算机及信息安全相关领域多年的专业积淀，将有力支撑网络空间安全本科专业的顺利开办与可持续发展。

2. 师资力量

计算机与人工智能学院现有一支结构合理、素质优良的师资队伍。为增强实践教学能力，学院还聘请了一批企业技术专家担任兼职教师。专任教师中“双师型”教师队伍初步建成。这支师资队伍能够满足应用型人才培养对教学和指导的需求。在网络安全方向，学院已有多名教师具备信息安全、密码学等专业背景或相关科研项目经验，可作为新专业的骨干力量。同时，学院将通过外聘行业资深专家、鼓励教师取得安全资格认证、选派教师进修培训等方式，不断充实和提升网络空间安全专业的师资水平，保障教学质量。雄厚的师资储备为专业建设提供了坚实的人才保障。

3. 实验教学条件

学院拥有完善的实验教学中心，配备了满足网络空间安全教学需要的实验室群。其中包含专门的信息网络安全实验室以及计算机网络工程实验室、仿真实训室等，与网络安全教学高度相关。实验中心设备先进、功能完备，既承担学院各专业的实验教学任务，也面向全校开出计算机公共课实践教学。实验教学队伍经验丰富、结构合理，能够指导学生开展网络攻防实训、安全测评等实践项目。依托现有实验平台，新专业可以开设密码学实验、网络攻防演练、系统安全配置等实践环节，实现理论与实践的紧密结合。完备的实验实训条件将确保学生获得充足的动手实践机会，培养解决实际安全问题的能力。

4. 校企合作资源

我校高度重视产教融合，已建立起稳定的校企合作网络，为网络空间安全专业的人才培养提供了丰富的实践平台和协同育人资源。学院地处武汉“光谷”核心区域，紧邻网络安全产业集群，这一地理优势使得我们与周边知名网络安全企业联系紧密、资源对接便捷。目前学院已与多家业内龙头企业共建实习实训基地，合作机制成熟。依托这些基地，学院在网络安全攻防、测评、运营等方向建有多个校外实践实训点，覆盖网络安全工作的各主要环节。学校推行“双导师制”，由企业工程师与校内教师联合指导学生实习，将企业真实项目引入教学，实现实战训练与课堂教学的深度融合。在项目驱动的实习模式下，学生参与企业实际安全项目全过程，实践成果还可用于毕业设计课题，做到学以致用。优质的校企合

作也为毕业生就业打通渠道。未来，我校将在网络空间安全专业继续深化产教协同：一方面，邀请企业安全专家参与课程共建、担任客座讲师；另一方面，与行业单位联合开发案例教材、举办技能竞赛和创新项目，以培养学生的实战能力和职业素养。丰富的校企合作资源和完善的协同育人机制，将有力保障网络空间安全专业人才培养质量和就业竞争力。

三、学校专业发展规划

1. 契合学校“十四五”发展规划

增设网络空间安全本科专业，符合学校中长期战略方向。我校将紧扣国家重大战略需求，着力发展新兴工科专业，优化学科专业结构，提升服务区域发展的能力。网络空间安全专业正是契合这一规划的新兴战略性专业。我校计划通过该专业的建设，完善计算机学科专业链条，实现相关学科的协同发展与交叉融合。与此同时，学校顺应“数字湖北”建设和中部地区信息产业升级的大趋势，将网络空间安全列为重点发展领域，以期为地方数字经济和社会治理提供人才与智力支持。增设本专业不仅丰富了学校学科门类，也是落实学校办学定位、打造优势特色专业群的重要举措，有助于提升学校的综合办学实力和社会影响力。

2. 对标“新工科”建设要求

当前高等工程教育正向“新工科”转型，强调学科交叉融合和实践创新人才培养。网络空间安全专业正是新工科背景下涌现的典型代表，其建设对标了教育部推进的新兴工程领域布局[16]。我校积极响应新工科建设，陆续开设了数据科学与大数据技术、人工智能等新兴专业，形成跨学科融合培养模式。网络空间安全专业的增设将进一步完善我校新工科专业集群。我们将在专业建设中贯彻新工科理念：例如，注重网络安全与人工智能、物联网、管理学等领域的交叉融合，培养复合型人才；强化实践教学环节，实施项目导向、案例驱动的教学改革；引入企业真实课题，培养学生的创新意识和工程实践能力。这些举措与新工科倡导的“厚基础、强实践、跨学科”培养要求高度一致。通过网络空间安全专业建设，我校将在新工科领域形成新的增长点和示范点，助力学校培养顺应未来产业变革的多层次复合型工程科技人才。

3. 服务应用型高校办学定位

武汉工程科技学院是一所应用型本科院校，始终坚持以服务区域经济社会发展为导向的人才培养定位。增设网络空间安全专业与学校应用型办学定位高度契

合，有助于强化我校服务地方、行业的能力。一方面，本专业培养的人才直接面向网络安全产业和数字经济建设一线，可为湖北省乃至中部地区的企事业单位提供急需的网络安全专门人才；另一方面，专业建设过程将加强校企合作和产学研结合，使教学内容紧贴产业实际，培养出的毕业生具备“下得去、留得住、用得上”的实战本领。这正体现了应用型高校培养高素质技术技能人才的目标。我校将充分发挥灵活办学机制，结合区域产业需求动态调整课程和实践内容，使网络空间安全专业成为服务地方的特色品牌专业。总之，网络空间安全本科专业的建设，将进一步凸显我校应用型人才培养的办学特色，为区域经济转型升级和社会安全保障贡献力量。

四、与现有专业的区分度

我校拟增设的网络空间安全本科专业与现有计算机类本科专业相比，在人才培养目标、课程体系、就业面向和核心能力等方面都有明确的差异化定位，避免了与兄弟专业的重复雷同。

（1）人才培养目标：现有的计算机科学与技术、软件工程、大数据等专业侧重于培养通用计算机技术人才，强调软件开发、数据处理或系统研发等广泛领域的能力。而网络空间安全专业则以培养网络安全专门人才为目标，着重塑造学生在网络安全防护、威胁情报分析、安全管理等方面的特长。例如，计算机科学与技术专业培养的是“宽口径”IT 工程师，具备软件开发和计算思维能力；而本专业培养的是精通安全技术的工程师，能够承担关键信息基础设施的安全保障和网络攻防任务。

（2）课程体系：各专业课程设置各有侧重。计算机科学与技术专业课程覆盖计算机原理、软件工程、数据库等基础广、偏重理论的软件和硬件知识；软件工程专业课程突出软件设计、项目管理和开发流程；大数据专业课程则集中于数据分析、机器学习和大数据平台技术。网络空间安全专业将构建安全领域特色课程体系，包括密码学、操作系统安全、网络攻击与防御、漏洞挖掘与渗透测试、安全编程、信息对抗等核心课程，这些课程在其它专业中仅作为选修或很少涉及[12]。同时，本专业课程强调实践训练，占比高，设置专业实验、网络攻防演练、信息安全管理实训等实践环节，从课程内容上保证学生获得系统全面的安全技能训练。

（3）就业面向：计算机类各现有专业毕业生的就业领域有所不同。计算机科学与技术和软件工程专业毕业生主要面向软件开发工程师、系统维护工程师、IT项目管理等岗位；数据科学与大数据专业毕业生则多从事数据分析师、大数据工程师等工作。而网络空间安全专业毕业生的就业方向集中在网络与信息安全领域，如安全运维工程师、网络安全工程师、渗透测试工程师、等级保护测评工程师、安全咨询顾问等。这些岗位对专业技能要求高度聚焦于安全领域，具有较强的专业特殊性。相较其他专业毕业生，网络空间安全专业学生在网络安全公司、信息安全服务机构、党政机关和企事业单位的信息安全岗位上更具竞争优势。本专业的增设将填补这一就业领域的空白，为学生提供新的就业增长点。

（4）核心能力：不同专业所培养的核心能力有所区别。现有计算机类专业侧重培养学生计算思维、编程开发、系统设计等通用能力，如算法设计能力、软件架构能力或数据处理能力。而网络空间安全专业侧重于培养学生安全防护与对抗的专项能力，包括安全漏洞发现与修补、网络入侵检测与响应、加密与解密、风险评估与安全策略制定等。这些核心能力具有高度的专业独特性，体现出网络空间安全学科“攻防兼备”的特点。通过本专业的学习，学生将形成系统全面的安全意识和技能体系，例如具备在复杂网络环境中分析安全威胁、设计安全解决方案、保障系统和数据安全的本领。因而，本专业培养的毕业生在核心能力上与其他专业拉开了明显差距，能够胜任更高要求的网络安全专门工作。

五、专业名称的规范性

我校申请增设的专业名称为“网络空间安全”，该名称严格符合教育部公布的本科专业目录规范，具有权威性和科学性[12]。一是名称规范一致：教育部《普通高等学校本科专业目录（2020版）》[13]将“网络空间安全”列为计算机类专业，专业代码080911TK，学制四年，授予工学学士学位[12]。可见，“网络空间安全”已成为全国高校统一采用的规范专业名称，使用该名称申报确保了与国家专业目录的一致性，符合教育主管部门对于专业命名的要求。我校将严格按目录使用规范名称，不使用任何生僻或夸大的表述，确保专业设置的严肃性和合法性。二是名称内涵科学：网络空间安全专业名称具有广泛的代表性和准确的指向性，能够科学概括本专业的学科内涵和培养领域。从学科范畴看，网络空间安全涉及密码学、计算机科学与技术、信息与通信工程、数学等多学科交叉领域[17]。名称中的“网络空间安全”涵盖了网络安全、信息安全、系统安全、数据安全等多个

层面的内容，反映出现代社会中维护网络空间主权和保障信息安全的综合要求。相较于早期的“信息安全”专业称谓，“网络空间安全”一词更全面、前沿，强调了国家主权维度和网络空间整体安全，比仅关注信息保密更具时代意义和科学性。教育部增设该专业名称（2015 年首次列入本科专业目录）也是为了顺应网络空间安全新领域的发展，体现专业建设与国家安全战略的紧密衔接。因此，采用“网络空间安全”作为专业名称[12]，既规范权威，又能够准确传达专业培养目标与内涵，易于社会和用人单位理解认同，具有很高的学科代表性。

综上，我校申报专业的名称和定位均严格遵循国家标准，名称规范、内涵科学，与本科专业目录保持一致。这将确保专业在批准设立后，所授学位和专业称号在全国范围内具有可比性和公信力，有利于毕业生的职业认同和行业认可。

六、专业建设的保障条件

为确保网络空间安全本科专业顺利建设和可持续发展，我校在经费投入、教学资源、校企协同和实践条件等方面制定了完备的保障措施:

（1）经费保障：学校承诺对新专业建设给予专项经费支持。专业获批后，将从年度预算中划拨充足资金，用于师资引进培养、实验室建设、课程开发及教材编写等。学校财务状况良好，教育投入持续增长，并能积极争取地方财政专项和行业合作经费支持专业发展。因此，在经费来源上有稳定保障，可持续满足专业建设需要。

（2）教学资源建设：学校已组织专家制定了网络空间安全专业的人才培养方案和课程大纲，完善了教学计划。后续将根据国家教学质量标准，建设一批核心课程和优质教材资源。同时，我们将充分利用现有计算机类专业的教学平台，共享通用基础课程，并针对本专业特点新开设网络安全法律法规、密码学等课程。教师教学发展中心也将为本专业教师提供培训，提升教学水平。图书馆和电子资源方面，目前已收藏有网络安全领域的专业书刊、数据库，并计划新增相关权威期刊和电子书，以支持教学与科研。通过持续的教学资源投入与建设，确保本专业学生“学有优教、教有优资”。

（3）校企协同育人：发挥我校产教融合优势，构建多方协同的人才培养机制。我们将依托已有的企业实训基地，邀请合作企业深度参与人才培养全过程。例如，联合企业制定人才培养方案和课程标准，使课程内容与行业需求同步更新；聘请行业资深工程师担任兼职教授或导师，讲授前沿技术、指导实践项目；与知

名网络安全企业合作共建“网络安全创新实验室”或“网络靶场”，作为学生实训和教师科研平台；开展订单式培养和企业奖学金计划，激发学生学业动力。通过校企“双主体”协同育人，保证本专业培养方案紧贴产业脉搏，学生的实践能力和职业素养符合企业用人标准。

（4）实习实践条件：学校高度重视实践教学环节，已为本专业搭建了多层次的实习实训体系。校内依托实验中心，可开展网络攻防演练、CTF竞赛等校内实践活动；校外依托共建基地，为每位学生提供不少于半年时间的企业实习机会。每个实习学生均配备校内导师和企业导师“双导师”联合指导，确保实习质量和安全。学校制定了完善的实习管理制度，包括实习前培训、过程跟踪和结果考评，将实践教学纳入学分体系严格管理。未来我们将继续拓展优质实习单位，加强实践教学条件，不断提高学生实践动手能力和就业竞争力。

综上所述，武汉工程科技学院在增设网络空间安全本科专业方面已经做好全面的保障准备。从资金到资源、从校内到校外，多方面的支持措施将确保专业建设起点高、运行稳、发展好。我们有信心依托学校现有的基础和优势，将网络空间安全专业打造成为符合国家战略需求、具备鲜明应用型特色的精品本科专业，为国家和区域输送大批高素质网络安全人才。

参考文献

[1] 中共中央办公厅，国务院办公厅. 国家网络空间安全战略[EB/OL]. 新华网，2016-12-27[2025-07-07].
http://www.xinhuanet.com/politics/2016-12/27/c_1120194459.htm.

[2] 国务院学位委员会，教育部. 关于增设网络空间安全一级学科的通知（学位〔2015〕11号）[EB/OL]. 中华人民共和国教育部政府门户网站，2015-06-03[2025-07-07].
http://www.moe.gov.cn/srcsite/A22/moe_843/201506/t20150603_189912.html.

[3] 教育部，国家发展改革委，财政部. 关于加强网络安全学科建设和人才培养的意见[EB/OL]. 中华人民共和国教育部政府门户网站，2016-09-25[2025-07-07].
http://www.moe.gov.cn/srcsite/A08/s7056/201609/t20160925_282542.html.

[4] 全国人民代表大会常务委员会. 中华人民共和国网络安全法[EB/OL]. 中国人大网，2016-11-07[2025-07-07].

http://www.npc.gov.cn/npc/c30834/201611/4a8616233d4c4e518712217d84f09d6f.shtml.

[5] 国务院. “十四五”国家信息化规划[EB/OL]. 中国政府网, 2021-12-27[2025-07-07]. http://www.gov.cn/zhengce/content/2021-12/27/content_5664874.htm.

[6] 国务院. “十四五”数字经济发展规划[EB/OL]. 中国政府网, 2022-01-12[2025-07-07]. http://www.gov.cn/zhengce/content/2022-01/12/content_5667977.htm.

[7] 中国信息通信研究院. 网络空间安全白皮书（2023年）[R/OL]. 中国信息通信研究院, 2023-09-07[2025-07-07]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202309/P020230907572797769974.pdf.

[8] 中国网络安全产业联盟. 中国网络安全产业发展报告（2023年版）[R]. 电子工业出版社, 2023年9月.

[9] 麦可思研究院. 2024年中国大学生就业报告[R/OL]. 麦可思研究院, 2024-06-12[2025-07-07]. https://www.mycos.com/article/detail/20240612100001.html.

[10] 中国信息安全测评中心. 中国网络安全人才发展白皮书(2022)[R/OL]. 中国信息安全测评中心, 2022-07-27[2025-07-07]. http://www.itsec.gov.cn/Data/View/2778.html.

[11] 湖北日报. 武汉：撑起“网络强国”的中部脊梁[N/OL]. 人民网湖北频道, 2023-05-20[2025-07-07]. http://hb.people.com.cn/n2/2023/0520/c192237-40423634.html.

[12] 教育部高等学校网络空间安全专业教学指导委员会. 高等学校信息安全专业指导性专业规范（第2版）[M]. 北京：清华大学出版社, 2021.

[13] 教育部高等教育司. 普通高等学校本科专业目录(2020年版)[EB/OL]. 中华人民共和国教育部政府门户网站, 2020-03-02[2025-07-07]. http://www.moe.gov.cn/srcsite/A08/s7056/202003/t20200302_426027.html.

[14] 中国新闻网. 网络安全人才需求升温 求职者期望平均月薪达14013元[N/OL]. 中国新闻网, 2021-04-29[2025-07-07]. https://www.chinanews.com/it/2021/04-29/9467517.shtml.

[15] Python84310366. 网络安全工程师前景怎么样？2024年网络安全行业分析[EB/OL]. CSDN博客, 2024-06-25[2025-07-07]. https://blog.csdn.net/Python84310366/article/details/144747755.

[16] 教育部. 关于加快建设高水平本科教育全面提高人才培养能力的意见（新时代高教40条）[EB/OL]. 中华人民共和国教育部政府门户网站, 2018-06-15[2025-07-07]. http://www.moe.gov.cn/srcsite/A08/s7056/201806/t20180615_340243.html.

[17] 中国科学技术信息研究所. 网络空间安全学科发展报告[R]. (注: 此为推测来源，具体报告名称和发布日期需查阅相关科研机构发布的报告)

10. 校内专业设置评议专家组意见表

校内专业设置评议专家组意见表

<table>
<tr><td colspan="2">总体判断拟开设专业是否可行</td><td>☑是　□否</td></tr>
<tr><td colspan="3">专业筹建负责人围绕网络空间安全专业的设立背景、行业发展趋势、人才培养需求、学科基础条件和未来建设规划作了详尽汇报。专家组认为，当前国家对网络空间安全高度重视，网络安全已上升为国家战略。随着数字经济、人工智能、工业互联网等新兴领域的发展，网络攻击日益复杂，数据安全、系统防护、密码应用等方面对专业技术人才的需求迅速增长。湖北省作为国家网络强省战略的重要支撑区域，在高校、科研机构、企事业单位中，对网络空间安全专业毕业生具有广泛且迫切的用人需求。
专家组实地查阅了学院师资队伍结构、实验教学平台、课程体系设计、产教融合实践基地建设等支撑条件。计算机与人工智能学院现已形成涵盖计算机科学与技术、软件工程、人工智能、物联网工程等方向的专业集群，专任教师中具备网络安全、信息安全、密码学等相关背景的博士和副高级以上职称人员比例较高，教学与科研能力强，梯队建设合理。学院建有信息网络安全实验室、虚拟化实训平台、攻防演练平台、大数据与人工智能实验室等，具备开设网络空间安全专业的基本实验条件，部分实验设备正在规划更新，未来可通过专项投入进一步完善。校外方面，已与多家网络安全企业、信息系统集成公司、公安信息化部门开展合作，初步具备稳定的实习实践基地支撑。
专家组一致认为，网络空间安全专业定位准确、设立依据充分、基础条件较为完备，具有良好的建设前景和人才培养基础。建议在专业正式设立后，进一步凝练特色方向，加强核心课程建设，推动高水平师资引进，强化实践教学条件建设，提升服务区域信息安全与产业发展的能力。
综上，专家组一致同意学校申报增设网络空间安全本科专业。</td></tr>
<tr><td colspan="2">拟招生人数与人才需求预测是否匹配</td><td>☑是　□否</td></tr>
<tr><td rowspan="3">本专业开设的基本条件是否符合
教学质量国家标准</td><td>教师队伍</td><td>☑是　□否</td></tr>
<tr><td>实践条件</td><td>☑是　□否</td></tr>
<tr><td>经费保障</td><td>☑是　□否</td></tr>
<tr><td colspan="3">专家签字：</td></tr>
</table>